Mikrokontrollerbasierendes bargeldloses Kassensystem mit RFID Leser

Diplomarbeit 2008

Höhere Fachschule Uster

© Philippe Villard 05-E (Elektronik) / 19.08.2008

Doku_DA.doc

1 Inhaltsverzeichnis

1 Inhaltsverzeichnis 1

2 Hinweise zur Dokumentation 5

2.1 Konventionen 5

2.2 Bezeichnung Datenträger 5

2.3 Bezeichnung der Legic Schreib- / Leseeinheit 5

3 Aufgabenstellung 6

4 Bestimmungen für die Diplomarbeit 7

5 Involvierte Personen 8

6 Management- Summary 9

6.1 Zweck 9

6.2 Grundsätzliches 9

6.3 Schwierigkeiten / spezielle Problemstellungen 9

6.4 Lösungsvorgehen 9

6.5 Gefundene Lösung 10

7 Vorabklärungen / Vorstudie 11

7.1 Zweck und Umfang der Vorstudie / Analyse 11

7.2 Zielsetzungen 11

7.3 Grundlagen RFID / Begriffe 11

7.4 Analyse von Bauteilen 12

7.5 Analyse von Entwicklungsumgebungen / (Mess-)Geräten 12

7.6 Analyse des bestehenden Marktes 12

7.6.1 Grundsätzliches 12

7.6.2 Vergleich 12

7.6.3 Fazit 12

7.7 Machbarkeit 12

7.8 Aufwandschätzung 12

8 Pflichtenheft 12

8.1 Grundsätzliches 12

8.2 Hardware 12

8.2.1 Übersicht 12

8.2.2 Gegeben 12

8.2.3 Zu erstellende Hardware 12

8.2.4 Human↔Machine Interface (HMI) 12

8.2.5 Speisung 12

8.3 Firmware 12

8.3.1 Entwicklungsumgebung 12

8.3.2 Erweiterbarkeit 12

8.4 Anforderungen an die Dokumentation *12*
8.4.1 Logischer Aufbau der Dokumentation 12
8.4.2 Bedienung / Inbetriebnahme des Gerätes 12
8.4.3 Datensicherheit 12

8.5 Testszenarien *12*

8.6 Zielsetzungen *12*
8.6.1 Mussziele für die geforderte Lösung 12
8.6.2 Wunschziele 12

8.7 Abweichungen und Korrekturen *12*

9 Persönliche Zielsetzungen 12

10 Zeitplanung Soll / Ist 12

10.1 Gesamtzeitplan *12*

10.2 Zeitplan Realisierung *12*

11 Hauptstudie / Konzept-Varianten 12

11.1 Zweck und Umfang der Hauptstudie *12*

11.2 Konzept- Varianten *12*
11.2.1 Begründung der Auswahl 12

11.3 Evaluation der einzelnen Komponenten *12*
11.3.1 Evaluation Mikrokontroller / Header Board 12
11.3.2 Begründung der Auswahl 12
11.3.3 Evaluation Display 12
11.3.4 Evaluation Tastatur 12
11.3.5 Begründung der Auswahl 12
11.3.6 Evaluation Entwicklungsumgebung 12
11.3.7 Begründung der Auswahl 12
11.3.8 Evaluation Speisungskonzept 12
11.3.9 Evaluation Signalgeber 12

12 Realisation / Umsetzung / Aufbau / Detailstudie 12

12.1 Zweck und Umfang der Realisation *12*

12.2 Realisierung Hardware *12*
12.2.1 Blockdiagramm 12

12.3 Schema *12*
12.3.1 uC Anschlüsse 12
12.3.2 Peripherie 12
12.3.3 Speisung 12

12.4 Erklärungen zum Schema *12*
12.4.1 Stromaufnahme 12
12.4.2 Toleranzrechnung / Toleranzüberlegungen 12

13 Realisierung der Software 12

13.1 Grundsätzliches *12*

13.2 main *12*

13.3 Beep *12*

13.4 Tastatur *12*

13.5 Nokia_lcd 12
13.6 Div_Funk 12
13.7 Leser 12
13.7.1 Befehl 12
13.8 Telegrammaufbau 12
13.9 Allgemein 12
13.10 Beispiel Benutzernummer lesen 12
13.11 State Event Diagramm 12

14 Datensicherheit 12

14.1 Grundsätzliches 12
14.2 Software bezogene Sicherheit 12
14.2.1 Authenticity (Authentizität) 12
14.2.2 Correctness (Korrektheit) 12
14.3 Hardware bezogene Sicherheit / Elektrische Sicherheit 12
14.3.1 Privacy (Datenschutz) 12
14.3.2 Emmission (Emissionen) 12
14.3.3 Immission (Imissionen) 12

15 Test / Messung / Verifikation 12

15.1 Testkonzept 12
15.1.1 Relevante Messgrössen / Parameter mit Toleranzen 12
15.1.2 Testbedingungen / Systemzustände 12
15.2 Testumsetzung 12
15.2.1 Testaufbau 12
15.2.2 Testgeräte 12
15.3 Testresultate 12
15.3.1 Gerät einschalten 12
15.3.2 Test BNR Lesen 12
15.3.3 Test Betrag lesen 12
15.3.4 Test Clear 12
15.3.5 Test Laden 12
15.3.6 Test Abwerten 12
15.4 Interpretation der Testresultate / Konsequenzen 12
15.5 Batterielebensdauer 12
15.6 Vergleich mit der Aufgabenstellung und Pflichtenheft 12
15.6.1 Gegenüberstellung der SOLL-IST-Grössen bzw. Parameter / Vergleich Mussziele 12
15.6.2 Gegenüberstellung der SOLL-IST-Grössen bzw. Parameter / Vergleich Wunschziele 12
15.6.3 Beurteilung und Fazit 12

16 Die Zukunft des bargeldlosen Kassensystems 12

17 Schlusswort 12

18 Installations-/Montageanleitung 12

18.1 Allgemeines 12
18.2 Installation und Montage des Gerätes 12
18.2.1 Abgleich HF Feld 12

19 Bedienungsanleitung 12

19.1 Allgemeine Informationen und Hinweise *12*

19.2 Inbetriebnahme *12*

19.3 Bedienung *12*
19.3.1 LADEN und ABWERTEN 12
19.3.2 CLEAR 12
19.3.3 ENTER 12
19.3.4 BETRAG LESEN 12
19.3.5 BNR LESEN 12
19.3.6 Funktionsübersicht 12

20 Glossar und Verzeichnisse **12**

20.1 Glossar *12*

20.2 Abbildungsverzeichnis *12*

20.3 Tabellenverzeichnis *12*

20.4 Quellenverzeichnis *12*
20.4.1 Literaturverzeichnis 12
20.4.2 Internetadressen 12

20.5 Stichwortverzeichnis *12*

21 Beilagen **12**

21.1 Beilagenverzeichnis *12*

22 Daten CD **12**

Der Anhang folgt ab Seite 65 und hat ein eigenes Inhaltsverzeichnis.

2 Hinweise zur Dokumentation

2.1 Konventionen

- `Quellcode ist in der Schriftart Courier New geschrieben`
- Internetadressen sind blau und unterstrichen www.homepage.com
- "Sätze, welche in "" geschrieben sind, sind Zitate von einer externen Quelle"

2.2 Bezeichnung Datenträger

Für ein RFID Medium gibt es verschiedene Bezeichnungen. In diesem Dokument werden die Bezeichnungen Datenträger und Tag verwendet. Weitere Bezeichnungen sind: Batch (umgangssprachlich), Schlüssel (allgemein), Chipkarte, Smartcard / Smart-Tag (englische Bezeichnung), RFID Karte etc.

2.3 Bezeichnung der Legic Schreib- / Leseeinheit

Die Legic Schreib-/ Leseeinheit wird in diesem Dokument der Einfachheit halber als Leser bezeichnet. "advant" ist die Bezeichnung für die Produktelinie von LEGIC, welche zum LEGIC RF- Standard und den ISO-Standards (15693, 14443) kompatibel ist.

3 Aufgabenstellung

Höhere Fachschule Uster

Herr
Phillippe Villard
Im Zelgli 7
8624 Grüt

Rapperswil-Jona, 21. April 2008

Diplomarbeit 2008

Sehr geehrter Herr Villard

Sie erhalten folgende Diplomarbeit zugeteilt, die selbständig zu lösen haben:

Mikrokontroller-basierendes bargeldloses Kassensystem mit RFID Leser

Beschreibung
Üblicherweise basieren Kassensysteme (z.B. in einer Mensa) auf einem Windowsrechner. Es wird eine Lizenz für ein Betriebssystem benötigt und die Kosten für die Hardware sind relativ teuer. Viele Funktionen des PC-Systems werden gar nicht benötigt.
Eine kleinere, auf Mikrocontrollerbasis erstellte Kasse, welche evtl. Batterie betrieben werden könnte, wäre sicherlich kostengünstiger und einfacher.

Aufgabenstellung
Entwickeln Sie einen Prototypen einer Kasse, welcher Geldbeträge auf einem RFID Smart-Tag auf und abbuchen kann. Entwickeln Sie das Gerät unter Einbezug Ihrer Kenntnisse über eine professionelle Projektabwicklung mit folgenden Teilaufgaben:

- Einarbeitung ins Gebiet und Abklärung der Realisierungsmöglichkeiten
- Erstellung eines Projektplans mit Aufgabenaufteilung
- Erstellung eines Pflichtenhefts mit Prioritäten
- Abklärungen bezüglich Datensicherheit (Authenticity, Correctness, Privacy, Emmission, Immission)
- Zusammenstellung der benötigten Entwicklungswerkzeuge
- Entwicklung einer Elektronik mit Mikrocontroller, RFID Leseeinheit Ansteuerung, Display, Tastatur
- Entwicklung einer Firmware welche die erwähnten Peripherien steuert
- Optional, Erweiterung der Systems um ein SD-Card basiertes Logging der Transaktionen
- Dokumentiertes Testen des erstellten Gerätes
- Erstellung einer Kurzbedienungsanleitung

Austeilung der Aufgabenstellung	Montag, 5. Mai 2008
Abgabe von 2 Dokumentationen	Dienstag, 19. August 2008

Freundliche Grüsse

Matthias Kläy

Höhere Fachschule Uster, Postfach 7, CH-8612 Uster, info@hfu.ch, www.hfu.ch
HFU Sekretariat, Haldenweg 10, 8322 Madetswil, Tel. 044 954 11 27, Fax 044 954 07 31

4 Bestimmungen für die Diplomarbeit

Die Bestimmungen sind der Internetseite der HFU zu entnehmen:

http://qms.bzu.ch/pdf/hfu/bestimmungen_vordiplom_diplomarbeiten.pdf

5 Involvierte Personen

Name	Funktion für die Diplomarbeit
Matthias Kläy	Betreuer
Noch nicht bekannt	Experte
Philippe Villard	Student HFU

Tabelle 1: Involvierte Personen

6 Management- Summary

6.1 Zweck

Dieses Kapitel beinhaltet eine kurze Zusammenfassung des Projekts, der Projektidee und des Ergebnisses der Arbeit.

6.2 Grundsätzliches

In der heutigen Zeit sind RFID Applikationen kaum mehr wegzudenken. Sei dies in der Zeiterfassung, Zutrittserfassung, in Produktionsabläufen, in Lieferketten, in der Identifizierung (zum Beispiel biometrischer Schweizer Pass 06) und so weiter oder eben im Bereich der bargeldlosen Bezahlung. Ein grosser Vorteil der RFID Technologie ist, dass das Auslesen und Zurückschreiben von Daten berührungslos gemacht werden kann. Es werden keine Verschleissteile mehr benötigt, die Wartung wird massiv vereinfacht, kann sogar zum Teil ganz weggelassen werden.
Seit neustem sind RFID Tags auch in Handys eingebaut. Diese Technologie heisst NFC (Near Field Communication), welche es erlaubt, RFID- Applikationen auf dem Handy herumzutragen und so z.B. mit dem Handy bargeldlos zu bezahlen.

Der Nutzen solcher bargeldloser Systeme ist eindeutig:
– hoher Komfort für den Anwender
– reduziertes Diebstahlrisiko, da sich kein Bargeld mehr im System befindet
– verloren gegangene Tags können gesperrt werden
– Reduktion der Betriebskosten

Die fast grenzenlosen Möglichkeiten sagen der RFID Technologie eine interessante Zukunft voraus. Diese Diplomarbeit geht vor allem auf die bargeldlose Bezahlung ein. In dieser Dokumentation werden auch Aussagen zur Sicherheit (HW+SW) sowie dem Datenschutz gemacht.

6.3 Schwierigkeiten / spezielle Problemstellungen

Bei neueren Technologien ist es meist schwierig, aussagekräftige und qualitativ gute Informationen zu bekommen. So auch bei der RFID Technologie. Die korrekte Ansteuerung eines Lesers ist nicht ganz einfach, da viele Abläufe und Fehlerquellen berücksichtigt werden müssen. Beispielsweise kann bei einem kontaktlosen System ein Tag jederzeit entfernt werden...

6.4 Lösungsvorgehen

Um ein Gerät zu entwerfen, welches von RFID Tags Geld ab- und aufwerten kann, muss man sich zuerst Gedanken zur Nutzung machen. Wie und wo soll das Gerät eingesetzt werden? Was muss das Gerät können? Dazu wurde ein Pflichtenheft erstellt.
Das Gerät muss somit zwingend über einen Display, eine Eingabetastatur sowie über ein Speisungskonzept verfügen. All diese Komponenten wurden durch Abwägen der Vor- und Nachteile sorgfältig ausgewählt.

6.5 Gefundene Lösung

In dieser Arbeit wurde ein so genanntes bargeldloses Kassensystem entwickelt, welches erlaubt Geldbeträge auf einem Legic RFID Tag beliebig bis zur Ladegrenze zu verändern. Zudem kann das Gerät gelesene Beträge auf einem Display ausgeben und, wenn vorhanden, eine Benutzernummer auslesen und ausgeben. Zudem wurden diverse Fehlerhandlings implementiert. Das Gerät erkennt zum Beispiel automatisch, wenn der Betrag, der geladen oder abgewertet wird zu klein oder zu gross ist (unter 0 SFr. oder über 110.- SFr.).

7 Vorabklärungen / Vorstudie

7.1 Zweck und Umfang der Vorstudie / Analyse

Um möglichst genaue und qualitativ gute Informationen zu sammeln waren einige Vorabklärungen nötig.

7.2 Zielsetzungen

Der Hauptgrund eine Vorstudie zu machen ist, grössere Probleme schon möglichst früh zu erkennen, diese dann zu analysieren und eventuell bereits frühzeitig zu lösen.

7.3 Grundlagen RFID / Begriffe

RFID steht für "Radio Frequency Identification". Es bezeichnet das Verfahren zur automatischen Identifizierung von Objekten über Funk. Ein solches System kann also berührungslos und ohne Sichtkontakt Daten über die Luft transportieren.
RFID- Systeme bestehen aus mindestens drei Komponenten: Softwaresystem, RFID- Tag (auch: RFID Transponder, Batch, Key etc. genannt) und Schreib-/ Leseeinheit (Leser).

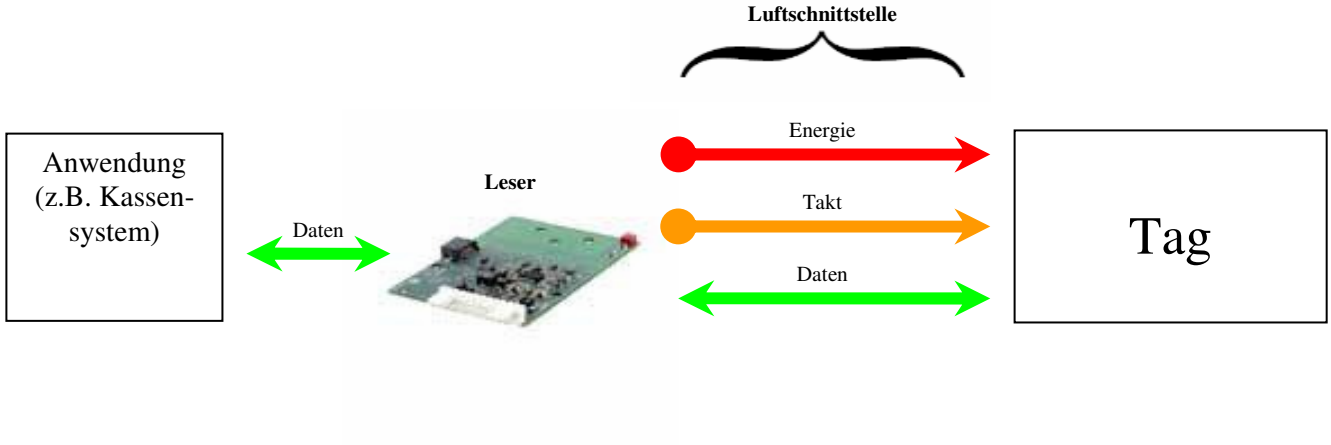


Abbildung 1: RFID -System

Ein Legic RFID- Transponder (Tag) besteht aus: Antenne, Mikrochip und Gehäuse. Er ist in vielen unterschiedlichen Gehäusearten erhältlich, zum Beispiel in Form von Schüsselanhängern oder Karten. Folgende Abbildung zeigt die Komponenten eines Tags in Kartenform:

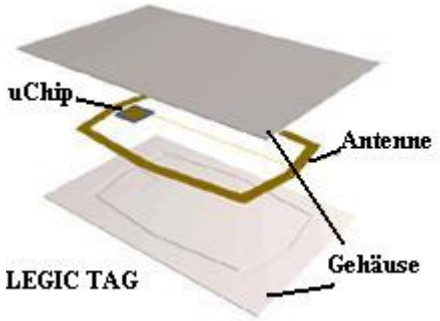


Abbildung 2: RFID Transponder (Tag)

Der Begriff "Transponder" ist zusammengesetzt aus den Begriffen Transmitter und Responder. Transponder können passiv oder aktiv sein. Legic Transponder sind grundsätzlich immer passiv.
Der Tag ist der mobile Teil des RFID- Systems. Er nimmt die von einer Leseeinheit gesendeten Signale auf und antwortet darauf. Tags sind die eigentlichen Datenträger eines RFID- Systems. Das Lesegerät versorgt den Tag über die so genannte "Luftschnittstelle" mit Energie für die Datenübertragung. Ein kleiner Kondensator im Tag lädt sich im HF-Feld auf und liefert so die Energie für den Mikrochip. Sobald ein Tag in die Nähe (Empfangsbereich) eines passenden Lesegerätes kommt, liest das Lesegerät die gespeicherten Daten kontaktlos aus. Legic Systeme arbeiten mit einer Frequenz von 13.56 MHz. So können im Normalgebrauch Lesedistanzen von ca. 5-20cm erreicht werden. Die Lesedistanz ist vor allem von der Antennengrösse des Tags und des Lesers abhängig.

7.4 Analyse von Bauteilen

Grundsätzlich werden, ausser dem Leser, keine ausserordentlich exotischen Teile benötigt. Mikroprozessoren sind heutzutage fast bei jedem Elektronikdistributor erhältlich. Lange Lieferzeiten könnten Probleme bereiten. Deshalb sind alle Teile möglichst früh zu bestellen.

7.5 Analyse von Entwicklungsumgebungen / (Mess-)Geräten

Für die einfache Programmerstellung wäre es von Vorteil, eine Entwicklungsumgebung zu haben, welche alle Aufgaben (Compiler, Assembler, Linker) beinhaltet. Varianten wären da zum Beispiel der IAR Compiler (IAR Embedded Workbench) oder ein GNU Compiler.

Für die Erstellung eines Gerätes ist ein normaler Elektronikarbeitsplatz ausreichend (Lötkolben, Oszilloskop, Multimeter, PC, kleiner Schraubstock, Netzgerät, diverse Zangen und Werkzeuge). Um ein Gehäuse anzufertigen werden eine Fräsmaschine, eine Bohrmaschine und ein Schleifband genügen.

7.6 Analyse des bestehenden Marktes

7.6.1 Grundsätzliches

Um die Marktlage zu analysieren müssen vorhandene Konkurrenzprodukte verglichen werden. Relevante Kriterien sind unter anderem: Preis, Stromverbrauch, Funktionen, Erweiterbarkeit.

7.6.2 Vergleich

Typ	**POS MobilePro**	**Max2**	**POS Color Touch**
Bild			
Hersteller	Vectron	Orderman	Vectron
Preis: (Wechsel-kurs: 1 € = 1.6165 SFr.)	Min. 1990 € (3216.84 SFr.)	ca. 1780 € ohne Leser (2877.37 SFr.)	ca. 4000 € (6466 SFr.)
Betriebsdau-er	4-10h	18h	Nur Netzbetrieb
Vernetzbar	Beschränkt	Beschränkt	Ja
Betriebs-System	Gerätespezifisch	"Windows 2000" oder "Windows NT4.0"	"Windows 2000" oder "Windows NT4.0"
Zusätzliche Optionen er-hältlich	Ja	Ja	Viele
Back Office Lösungen	Vorhanden	Vorhanden	Vorhanden
Mobilität	Sehr hoch	Sehr hoch	keine
Option Legic Leser mög-lich	Nein	Ja	Ja

Tabelle 2: Vergleich Markt

7.6.3 Fazit

Auf dem Markt bestehen sehr viele verschieden Kassenterminals. Es fällt auf, dass die Geräte ziemlich teuer sind. So kostet das günstigste Gerät das ich gefunden habe 2877.37 SFr. Eine stolze Summe für ein so kleines Gerät, das "nur" Statistiken verwalten und anzeigen kann...
Neben den oben verglichenen Geräten gibt es natürlich noch eine Vielzahl anderer Geräte. Billigkassen ohne bargeldloses Zahlungssystem sind zum Teil schon ab 500 SFr. erhältlich.

7.7 Machbarkeit

Für die Entwicklung eines bargeldlosen Zahlungssystems bedarf es folgender Komponenten:

- Speisungskonzept	⇒ Einfach realisierbar
- Kenntnisse RFID	⇒ zum Teil vorhanden Buch: RFID&Co. ISBN 3-7723-5120-4
- Kenntnisse Mikrokontroller	⇒ von MC1+MC2 vorhanden
- Kenntnisse einer Programmiersprache	⇒ "C" von MC1+MC2 vorhanden
- Schema	⇒ muss erstellt werden
- Gehäuse	⇒ kann simpel sein (Prototyp)
- Zeitplan / Schätzung	⇒ muss erstellt werden
- Pflichtenheft	⇒ muss erstellt werden
- Eventuell Development Board	⇒ muss evaluiert werden
- Diverse Komponenten wie Tastatur, Display	⇒ müssen evaluiert werden

7.8 Aufwandschätzung

Arbeit	**Zeit [h]**	**KW 19**	**KW 20**	**KW 21**	**KW 22**	**KW 23**	**KW 24**	**KW 25**	**KW 26**	**KW 27**	**KW 28**	**KW 29**	**KW 30**	**KW 31**	**KW 32**	**KW 33**	**KW 34**	**KW 35**
Informationen sammeln	10																	
Planung	15																	
Lösungsvarianten suchen	10																	
Evaluation uC / Entwick-lungsumgebung	15																	
Realisierung	70																	
Tests	10																	
Allfällige Verbesserungen	15																	
Doku	55																	
Präsentation vorbereiten	10																	
Aufwand Total	**210**																	
Meilensteine																		
Beenden der Planungsphase																		
Beenden Evaluation uC																		
Beenden Realisierungsphase																		

Tabelle 3: Aufwandschätzung

8 Pflichtenheft

8.1 Grundsätzliches

Es soll ein Prototyp entwickelt werden, welcher es erlaubt Geldbeträge auf LEGIC Transponder Chips zu verändern. Folgendes Pflichtenheft entstand aus der Aufgabenstellung für die Diplomarbeit 2008. Das System soll die unten aufgeführten Anforderungen erfüllen:

8.2 Hardware

8.2.1 Übersicht

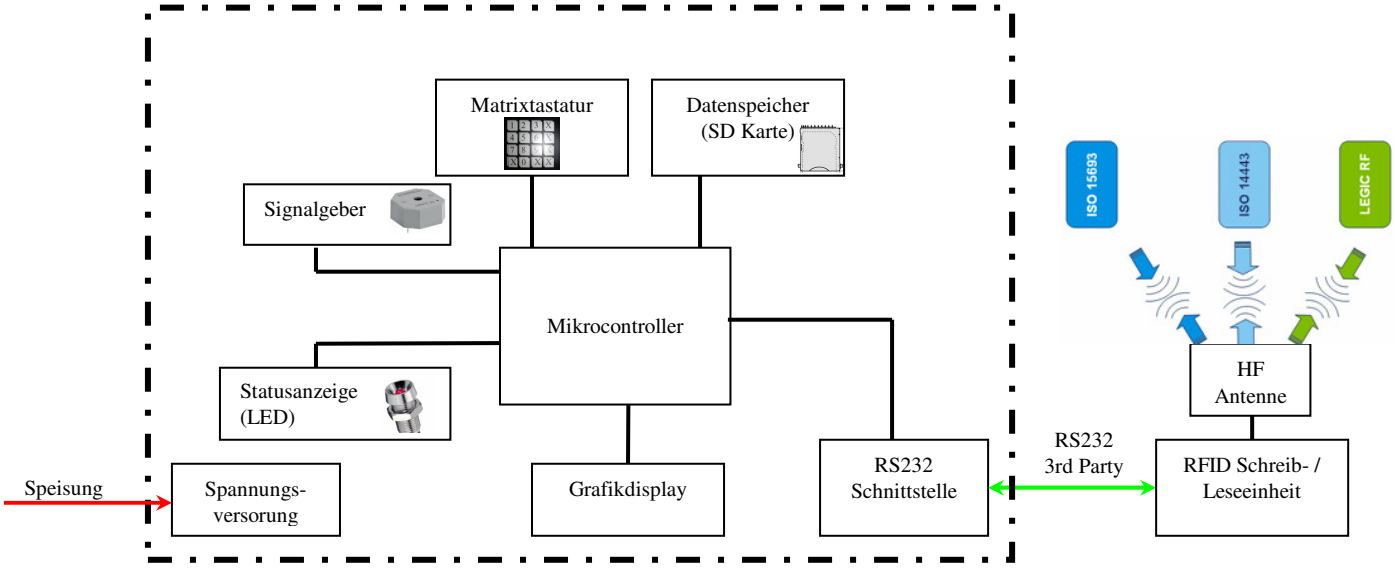


Abbildung 3: Übersicht Hardware

8.2.2 Gegeben

Als RFID Schreib-/Leseeinheit soll eine Troll advant V24 Einbauplatine der Firma EVIS AG verwendet werden. Dieser RFID Leser kann über eine serielle Schnittstelle (RS232) mit dem 3rd-Party Protokoll angesteuert werden. Die HF Antenne ist abtrennbar. Für die Softwareanbindung wird auf die Protokollbeschreibung (Kommunikations- Protokoll EVIS 3rd Party SERPROT8) der Firma EVIS AG verwiesen. Auf dem Leser ist das Security Chip Set multi- standard SC-2560 der Firma Legic integriert. Der Leser wird mit 5V DC betrieben.

8.2.3 Zu erstellende Hardware

Die Hardware besteht aus verschiedenen Komponenten. Für die Entwicklung der Hardware soll ein Schema gezeichnet werden. Es ist ein Prototyp zu erstellen, welcher z.B. auf einer Europakarte aufgebaut und in ein geeignetes Gehäuse gebaut werden kann. Das Gerät soll unter normalen klimatischen Bedingungen betriebsfähig sein (Temperatur: 5°C-50°C, Luftfeuchtigkeit: ~20%-95%).

8.2.4 Human↔Machine Interface (HMI)

Eingabe

Eingabe	Funktion	Umsetzung
Gerät einschalten	Gerät wird eingeschaltet	Schalter am Gehäuse
Umschalten zwischen Batterie und externer Speisung	Es wird von externer Speisung auf die interne Batterie umgeschaltet	Schalter am Gehäuse
Geldbetrag	Ladebetrag resp. abzuwertender Geldbetrag wird eingegeben	Bedientastatur (Matrixtastatur 0-9, „Eingabe“, Abwerten, Laden)
Löschen der Eingabe	Ein eingegebener Geldbetrag wird wieder gelöscht	Bedientastatur (Matrixtastatur „Löschen“)

Tabelle 4: Human↔Machine Interface Eingabe

Ausgabe

Ausgabe	Umsetzung
Speisung 5V DC ein	LED grün
Speisung 3.3V DC ein	LED grün
Karte in Feld	LED orange
Status LED	LED orange
Geldbetrag wurde erfolgreich abgezogen	Signalgeber
Anzeige des zu buchenden Geldbetrages, Anzeige vorhandenes Guthaben auf dem Tag	Grafik Display

Tabelle 5: Human↔Machine Interface Ausgabe

8.2.5 Speisung

Allgemein ist darauf zu achten, dass die ganze Anwendung möglichst wenig Energie braucht. Dies nicht zuletzt um sie mit Batterie oder Akku betreiben zu können. Es soll zwischen Netz- und Batteriebetrieb umgeschaltet werden können.

8.3 Firmware

Mit Hilfe eines Mikrokontrollers soll der Leser angesteuert werden (Kommunikations-Protokoll EVIS 3rd Party SERPROT8). Es müssen nicht alle Befehle implementiert werden. Grundsätzlich soll die Software modular aufgebaut werden (in Form von Modulen und Funktionen). Es ist ein Systemdesign zu realisieren, welches in überschaubare Teilgebiete gegliedert werden kann. Diese sollen zueinander möglichst wenige Berührungspunkte haben und möglichst eigenständig sein. Wo möglich und sinnvoll sollen auch Funktionen zur Datensicherheit implementiert werden. Ein Struktogramm soll eine Übersicht über die Software geben. Die Software soll in der Hochsprache C geschrieben werden.

8.3.1 Entwicklungsumgebung

Es soll eine geeignete Entwicklungsumgebung für den gewählten Mikrokontrollertypen gewählt werden. Für das effiziente Arbeiten soll eine Entwicklungsumgebung wenn möglich ganzheitlich sein (Editor, Compiler, Debugger etc. in einem).

8.3.2 Erweiterbarkeit

Sollte die Implementation einer SD Kartenansteuerung aus zeitlichen Gründen nicht realisierbar sein, so sollen zumindest Hardware- und Software- Vorkehrungen für eine mögliche spätere Integration getroffen werden.
Die Firmware soll so ausgelegt sein, dass eine unterschiedliche Behandlung von Benutzerkategorien möglich gemacht werden könnte. Dies kann zum Beispiel bei einem prozentualen Preisabschlag (je nach Benutzergruppe) notwendig sein.

8.4 Anforderungen an die Dokumentation

Weitere Anforderungen sind den Bedingungen zur Diplomarbeit zu entnehmen.

8.4.1 Logischer Aufbau der Dokumentation

Die Dokumentation soll sauber und übersichtlich gegliedert werden. Informationen sollen mittels Stichwort und/ oder Inhaltsverzeichnis möglichst rasch gefunden werden.

8.4.2 Bedienung / Inbetriebnahme des Gerätes

Für das zu erstellende Gerät selbst ist eine kurze Bedienungsanleitung zu erstellen damit auch ein Laie das Gerät bedienen kann.

8.4.3 Datensicherheit

Es sind Abklärungen bezüglich Datensicherheit (Authenticity, Correctness, Privacy) und elektrischer Sicherheit (Emmission, Immission) zu beschreiben.

8.5 Testszenarien

Die Testszenarien sollen wichtige Punkte für den Test des ganzen Systems und deren einzelner Komponenten beinhalten. Die Funktionalität der Hardware und der Software sollen anhand des Pflichtenhefts geprüft werden.

8.6 Zielsetzungen

8.6.1 Mussziele für die geforderte Lösung

Beschreibung	Priorität (1 = Höchste, 3 = Niedrigste)
Laden und Abwerten von Beträgen	1
Anzeige der Transaktionen auf einem Display	1
Eingabe der Geldbeträge über eine Tastatur	2
Erweiterbarkeit des Systems (elektrische Erweiterbarkeit, verschiedene Preiskategorien etc.)	2
Abklärungen betreffend Datensicherheit (Authenticity, Correctness, Privacy, Emmission, Immission)	2
Optische Darstellung (LED) über Betriebszustand	3
Akustisches Signal bei einer Auf-/Abbuchung	3

Tabelle 6: Mussziele

8.6.2 Wunschziele

Beschreibung	Priorität (1 = Höchste, 3 = Niedrigste)
Logfile auf eine SD Karte	1
Implementation Dateisystem um auf die SD Karte zu schreiben	2
Anzeige Batteriezustand	3

Tabelle 7: Wunschziele

8.7 Abweichungen und Korrekturen

Gegenüber der Aufgabenstellung haben sich keine Abweichungen ergeben.

9 Persönliche Zielsetzungen

Mein persönliches, oberstes Ziel ist es, möglichst viel zu lernen. Ich möchte meine in der HFU gelernten Fähigkeiten einerseits im fachlichen andererseits im projektorientierten Arbeiten umsetzen und Neues erlernen.
Des Weiteren möchte ich während der Zeit der Diplomarbeit meine persönliche Belastbarkeit noch besser kennen lernen und mich selbst beobachten bei der erhöhten geistigen Beanspruchung (Schule, Diplomprüfungen, 100% Arbeitspensum, Diplomarbeit etc.).

10 Zeitplanung Soll / Ist

10.1 Gesamtzeitplan

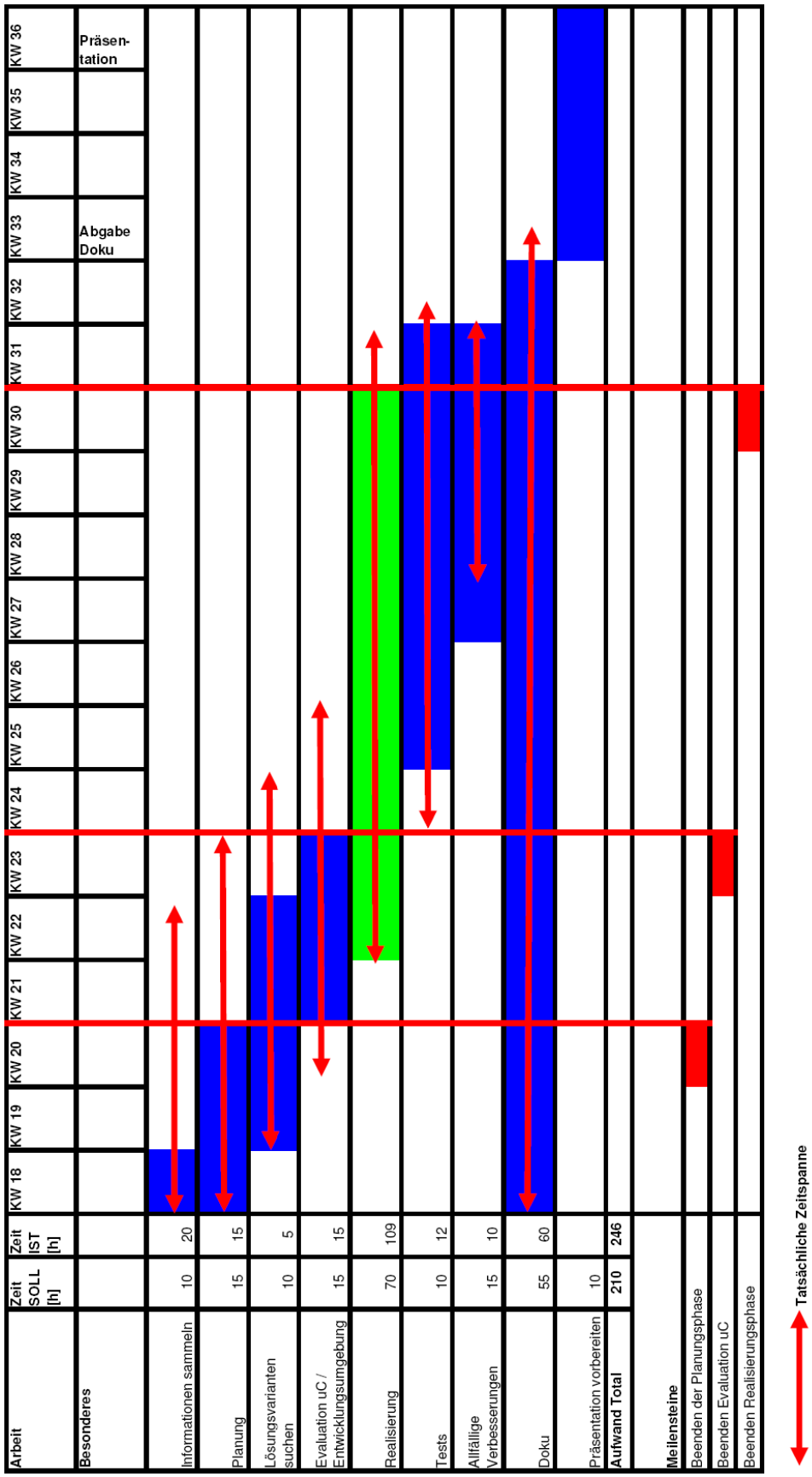
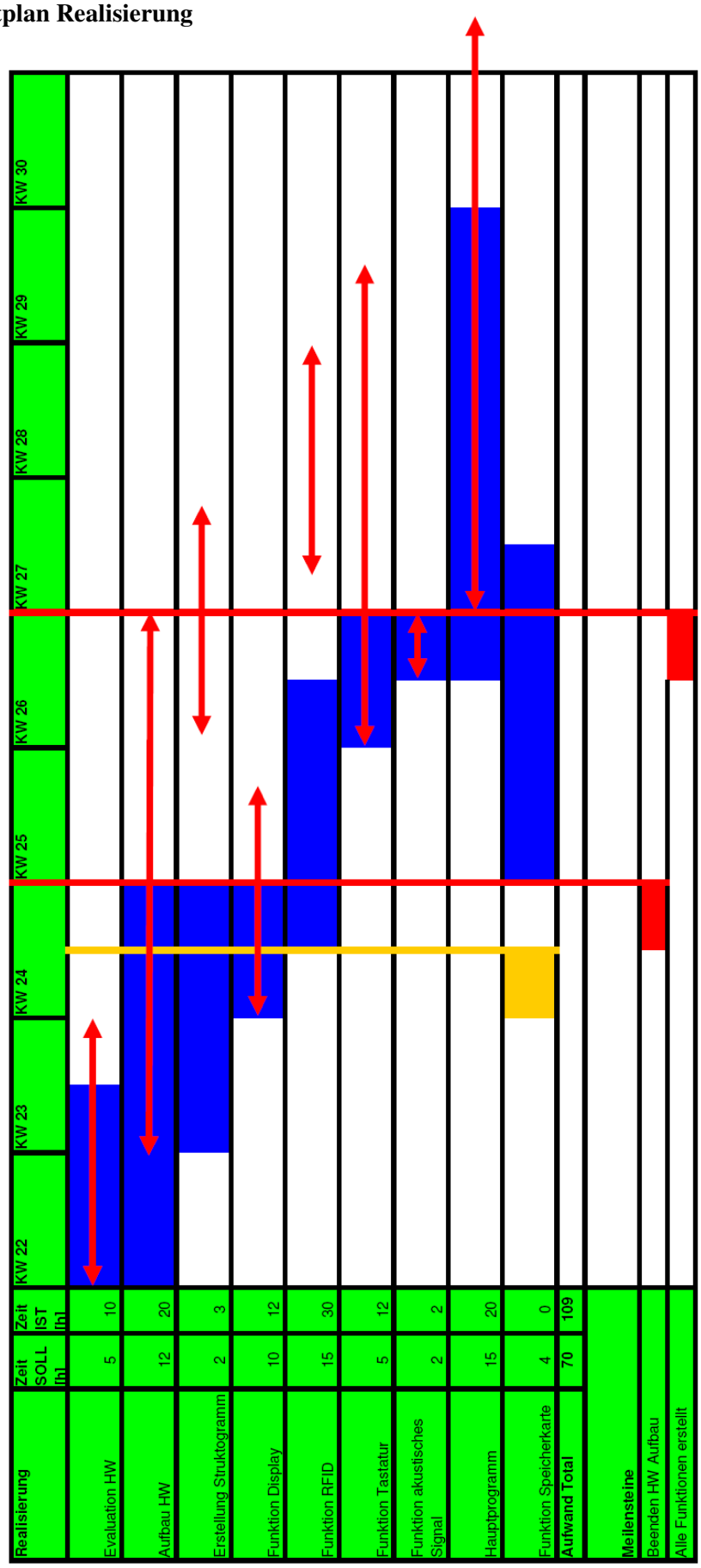


Tabelle 8: Gesamtzeitplan

10.2 Zeitplan Realisierung



Realisierung	Zeit SOLL [h]	Zeit IST [h]
Evaluation HW	5	10
Aufbau HW	12	20
Erstellung Struktogramm	2	3
Funktion Display	10	12
Funktion RFID	15	30
Funktion Tastatur	5	12
Funktion akustisches Signal	2	2
Hauptprogramm	15	20
Funktion Speicherkarte	4	0
Aufwand Total	70	109
Meilensteine		
Beenden HW Aufbau		
Alle Funktionen erstellt		

Tabelle 9: Zeitplan Realisierung

11 Hauptstudie / Konzept-Varianten

11.1 Zweck und Umfang der Hauptstudie

Um die optimalen Komponenten für die Erstellung des Prototyps zu evaluieren ist es notwendig einzelne Varianten zu vergleichen. Auf die gewählten Komponenten / Lösungswege wird im Kapitel Realisation / Umsetzung / Aufbau / Detailstudie detaillierter eingegangen.

11.2 Konzept- Varianten

Folgende Varianten standen zur Auswahl:

Variante	Vorteile	Nachteile	Besonderes
Header Board	- Sehr hoher Lerneffekt - Flexible Gestaltung - Viele Möglichkeiten - Gut erweiterbar	- Hoher HW Aufwand - Zeitintensiver HW Aufbau	
Fremdes Develop-ment Board	- hoher Lerneffekt - geringer HW- Aufwand	- Gehäuse nicht möglich - nicht sehr flexibel - Schwierige Evaluation für erforderliche Peripherie	
H8 Board	- geringer HW- Aufwand	- Nicht flexibel - geringerer Lerneffekt - Gehäuse nicht möglich	- Bereits durch den Unterricht MC1+MC2 bekannt

Gewählte Variante

Tabelle 10: Konzeptvarianten

11.2.1 Begründung der Auswahl

Die Vorteile beim Einsatz eines Header Boards überwogen den anderen beiden Varianten klar. Die einzigen Nachteile (hoher HW- Aufwand und zeitintensiv) der Header Board Variante werden durch die Vorteile (sehr hoher Lerneffekt, flexible Gestaltung, viele Möglichkeiten, gute Erweiterbarkeit) überwogen. Vor allem die Flexibilität und die gute Erweiterbarkeit für eine spätere Anbindung weiterer Komponenten gaben den Ausschlag.
Header Boards sind für die meisten Mikrokontrollertypen zu haben.

11.3 Evaluation der einzelnen Komponenten

11.3.1 Evaluation Mikrokontroller / Header Board

Anforderungen:

- viele gute Informationen vorhanden
- mindestens 2 UARTs
- geringer Stromverbrauch (Batteriebetrieb)

Folgende 3 Mikrokontrollertypen standen zur Auswahl:

Variante	Vorteile	Nachteile	Features
MSP430F169 TEXAS INSTRUMENTS	- Sehr verbreitet - Viele Informationen im Internet verfügbar - Hoher Lerneffekt - Einfacher Low Power Modus	- Einarbeitung	- 16-bit RISC CPU - 60K Bytes Program Flash - 48 I/O Pin
H8 3076 F RENESAS Everywhere you imagine.	- Bereits durch den Unterricht MC1 und MC2 bekant - Entwicklungsumgebung vorhanden	- Eher veraltet	- 32-Bit CPU (8*32 Reg.) - 128kB on-chip Flash - 70 I/O Pin
ARM 7 sam7x256 ATMEL Everywhere You Are®	- Sehr verbreitet - Viele Informationen im Internet verfügbar	- Hohe Komplexität - Eher überdimensioniert - Einarbeitung	- 32Bit - 256kB Speicher - 66 I/O Pin

Gewählte Variante

Tabelle 11: Evaluation Mikrokontroller

11.3.2 Begründung der Auswahl

Der MSP430 Kontroller mit der klassischen Von-Neumann-Architektur ist in vielen Ausführungen mit leistungsfähiger Peripherie verfügbar. Ich entschied mich für den F169, weil er auch eine gewisse Erweiterung meiner Anwendung ermöglicht. Die Geschwindigkeit des Kontrollers hatte für die Evaluation keinen Einfluss, da diese in dieser Anwendung nicht kritisch ist. Gegen den H83076F sprach vor allem, dass er eher veraltet ist. Die überdimensionierte Performance für die Anwendung in dieser Diplomarbeit sprach gegen den ARM7.

11.3.3 Evaluation Display

Anforderungen:

- gut ablesbar
- geringer Stromverbrauch
- wenn möglich mit Hintergrundbeleuchtung
- einfach ansteuerbar
- eventuell grafische Darstellungen

Variante	Vorteile	Nachteile
Nokia 3310 Grafikdis-play	- Grafische Darstellungen möglich - Hintergrundbeleuchtung möglich - Geringer Stromverbrauch	- Evtl. schwierigere Ansteuerung (SPI) - Relativ klein
LCD-Textdis-play	- Einfach ansteuerbar - Einfache Hintergrundbeleuchtung	- Grafische Erweiterungen / Spielereien schlecht möglich - Nur eine relativ geringe Anzahl Zeichen mög-lich

Gewählte Variante

Tabelle 12: Evaluation Display

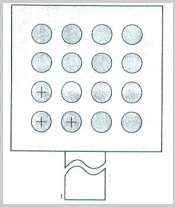
Ich habe mich für ein Nokia 3310 LCD Grafikdisplay mit einem Philips PCD8544 Controller entschieden. Es hat eine 84 * 48 Pixel Auflösung. Es unterstützt die Standard SPI Kommunikation und ist dank dem geringen Stromverbrauch für batteriebetriebene Anwendungen sehr gut geeignet. Weitere Angaben zum Kontroller und der Ansteuerung sind dem Datenblatt auf der Beilagen- CD zu entnehmen.

11.3.4 Evaluation Tastatur

Anforderungen:

- mindestens 16 Tasten
- Wenn möglich aufklebbar
- Wenn möglich selber "designbar"

Folgende beiden Tastaturen standen zur Auswahl:

Variante	Vorteile	Nachteile	Features
PKM-16 	- Taste mit Metallknackfrosch - Rückseite selbstklebend - Individuelle Beschriftung durch handelsübliche Folie möglich - Geringe Masse (einfache Montage auf Kleingehäuse)	- benötigt eine gerade Unterlage	- Lebensdauer: 1 Mio. Schaltzyklen
ECO 16250 06	- Bereits durch den Unterricht MC1 und MC2 bekannt	- Keine individuelle Beschriftung möglich - Nicht aufklebbar	

Gewählte Variante

Tabelle 13: Evaluation Tastatur

11.3.5 Begründung der Auswahl

Die Vorteile der Folientastatur PKM-16 sind offensichtlich. Ausschlaggebend für die Wahl der PKM-16 war unter anderem dass sie individuell beschriftbar ist (es gibt auf der Welt kaum eine Tastatur, welche mit den Ziffern 1-9 und den Tasten "Laden", "Abwerten", "Clear", "Enter", "Betrag lesen" und "BNR Lesen" bezeichnet ist...).

11.3.6 Evaluation Entwicklungsumgebung

Folgende beiden Entwicklungsumgebungen standen zur Auswahl:

Variante	Vorteile	Nachteile
IAR	- Weit verbreitet - Einfache Handhabung - Schneller, kompakter Code	- Codebegrenzung auf 4kBytes oder 30 Tage Test (sonst sehr teuer)
GCC	- Kostenlos - Weit verbreitet	- Eher schwierige Installation - Code größer als bei IAR

Gewählte Variante

Tabelle 14: Evaluation Entwicklungsumgebung

11.3.7 Begründung der Auswahl

Der ausschlaggebende Punkt bei der Wahl einer Entwicklungsumgebung war die einfache Handhabung und Installation der IAR Entwicklungsumgebung. Beim GCC wäre die Installation möglicherweise sehr zeitaufwändig gewesen, obwohl es im Internet relativ viele Anleitungen gibt.
Um keine teure IAR Lizenz kaufen zu müssen wurde eine Codegrössenabschätzung gemacht. Um zu prüfen, wie gross das Programm wird muss unter Projektoptionen / Linker unter dem Tab Listing ein Häkchen bei "Generate linker Listing" und "Generate modul summary" gesetzt und HTML angewählt werden. So wird ein HTML File generiert, welches zuunterst anzeigt, wie gross das Programm ist (CONST memory+ CODE memory= ROM Platzbedarf, DATA memory = RAM Platzbedarf). Mein Test ergab, dass CONST memory keinen Einfluss auf die Begrenzung hat. Die einzelnen Funktionen können also ohne weiteres mit der 4k Bytes begrenzten Version entwickelt werden. Eventuell muss gegen Ende der Programmierphase die 30 Tages Testversion, welche keine Codebegrenzung hat, verwendet werden.

11.3.8 Evaluation Speisungskonzept

Anforderungen:

- Muss mit 9V Batterie 6LR61 arbeiten können
- Batterie muss einfach austauschbar sein
- 3.3 VDC Speisung für uC
- 5VDC Speisung für RFID Leser

Für die Realisation der Speisung habe ich mich für Linear Regler 1117 von National Semiconductor entschieden.

11.3.9 Evaluation Signalgeber

Als Signalgeber wird ein gewöhnlicher Miniatur-Signalgeber verwendet, da eine einfacher "Piepston" vollkommen ausreicht. Es muss keine Musik abgespielt werden können...

12 Realisation / Umsetzung / Aufbau / Detailstudie

Unter Realisation wird einerseits die Detailspezifikation in Form von Blockdiagrammen und Struktogrammen inklusive Schema ausgehend vom Konzept und der ausgewählten Lösungsvariante verstanden. Andererseits wird auch die konkrete Umsetzung in HW (Aufbau) oder SW (Codierung) verstanden.

12.1 Zweck und Umfang der Realisation

Es wird ein lauffähiges Gerät aufgebaut. Da es ein Prototyp ist reicht es aus wenn es auf einer Europaplatine aufgebaut wird. Für die Verbindung der einzelnen Komponenten wird Lackdraht verwendet. Die Platine ist in ein Gehäuse eingebaut.

12.2 Realisierung Hardware

12.2.1 Blockdiagramm

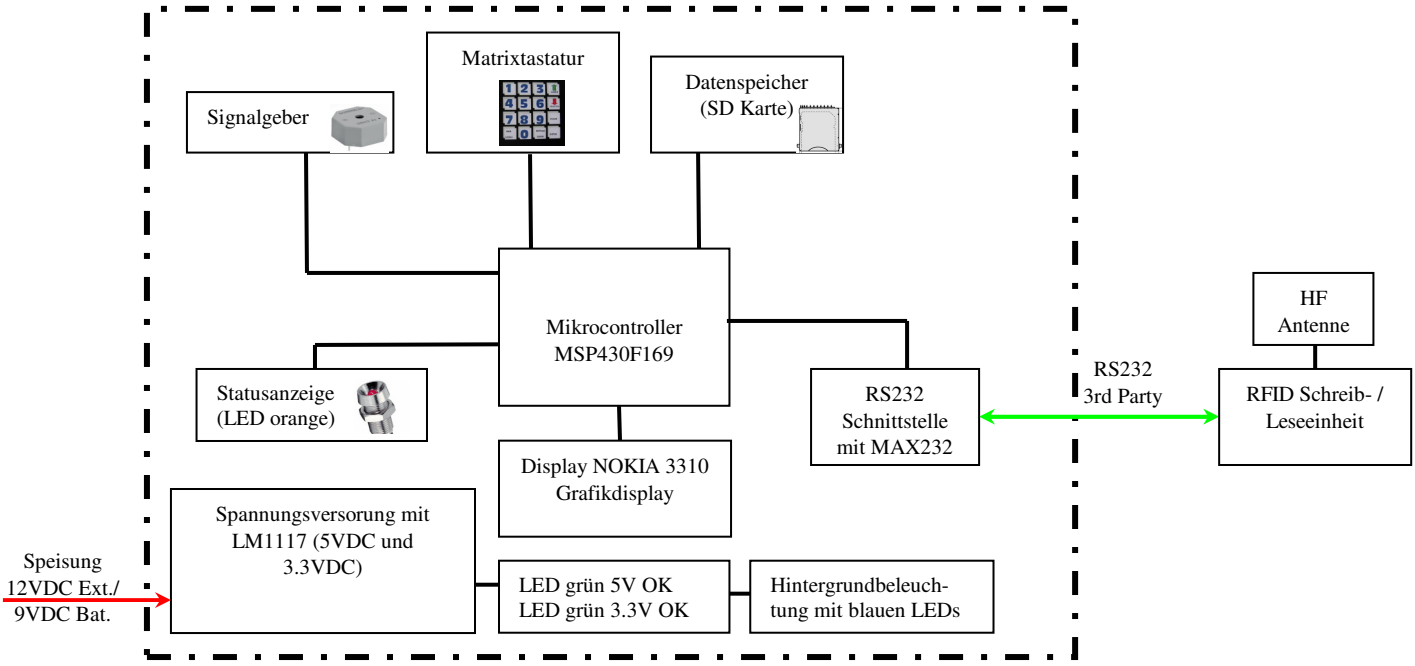
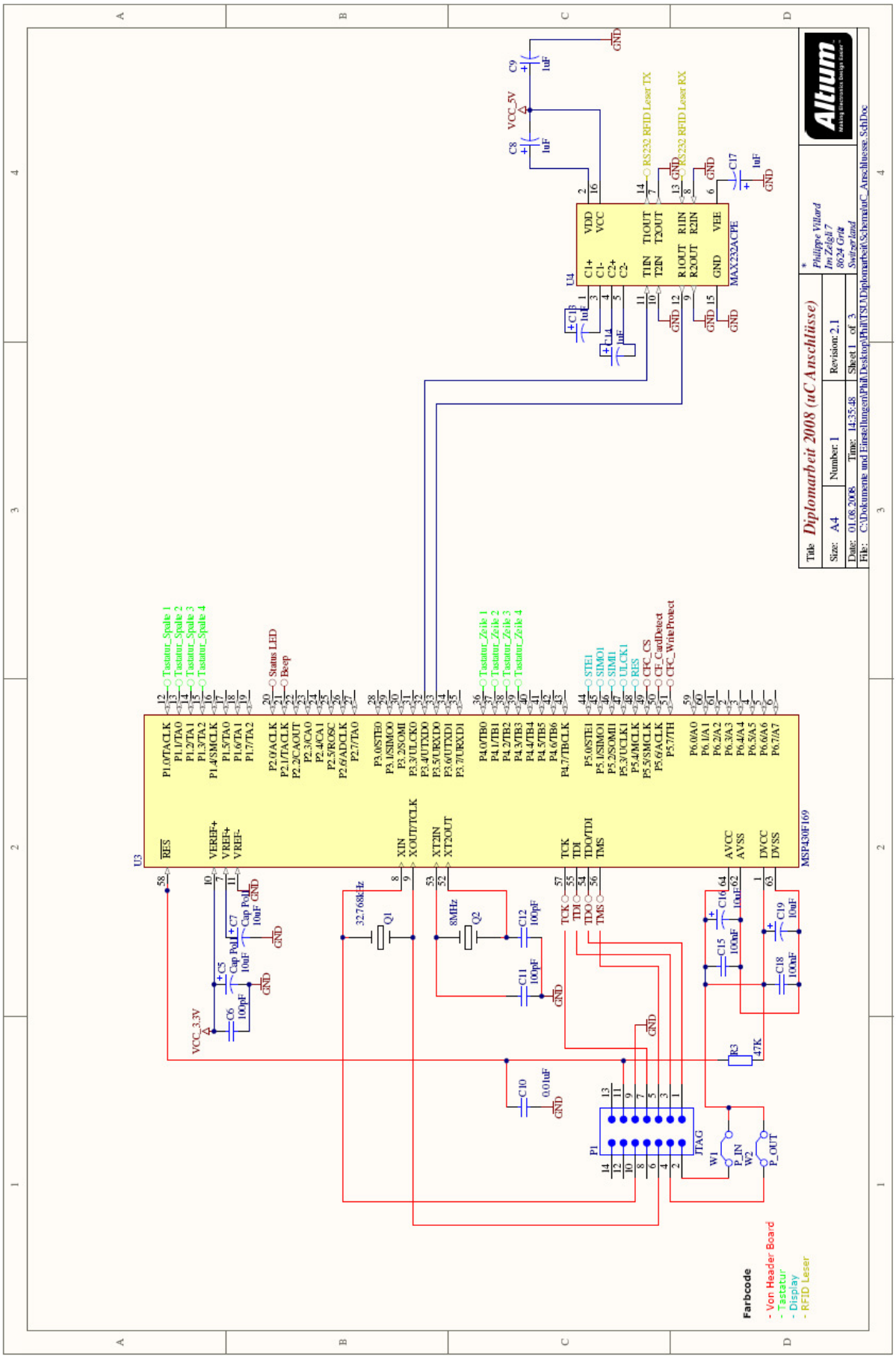


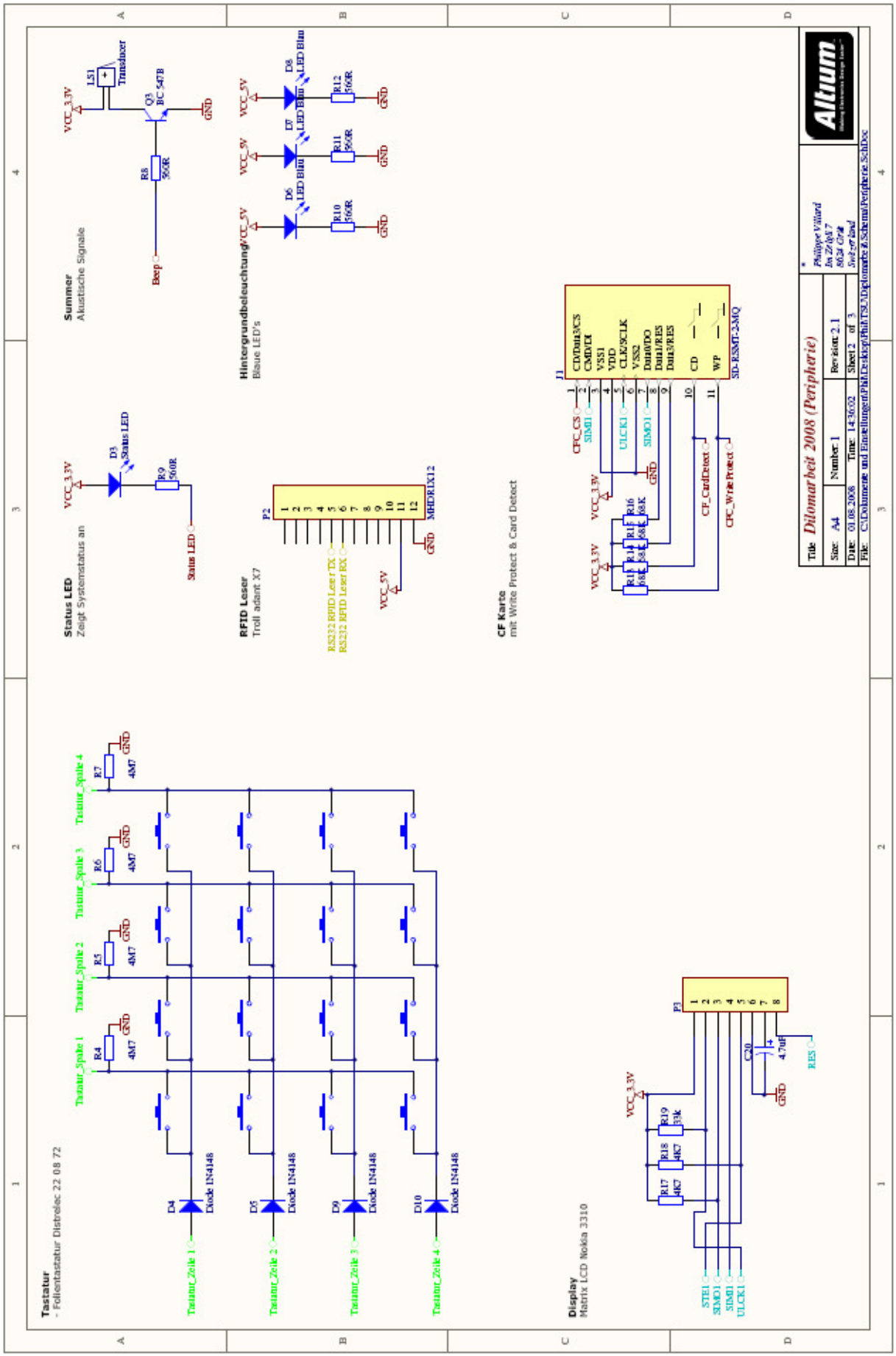
Abbildung 4: Blockdiagramm

12.3 Schema

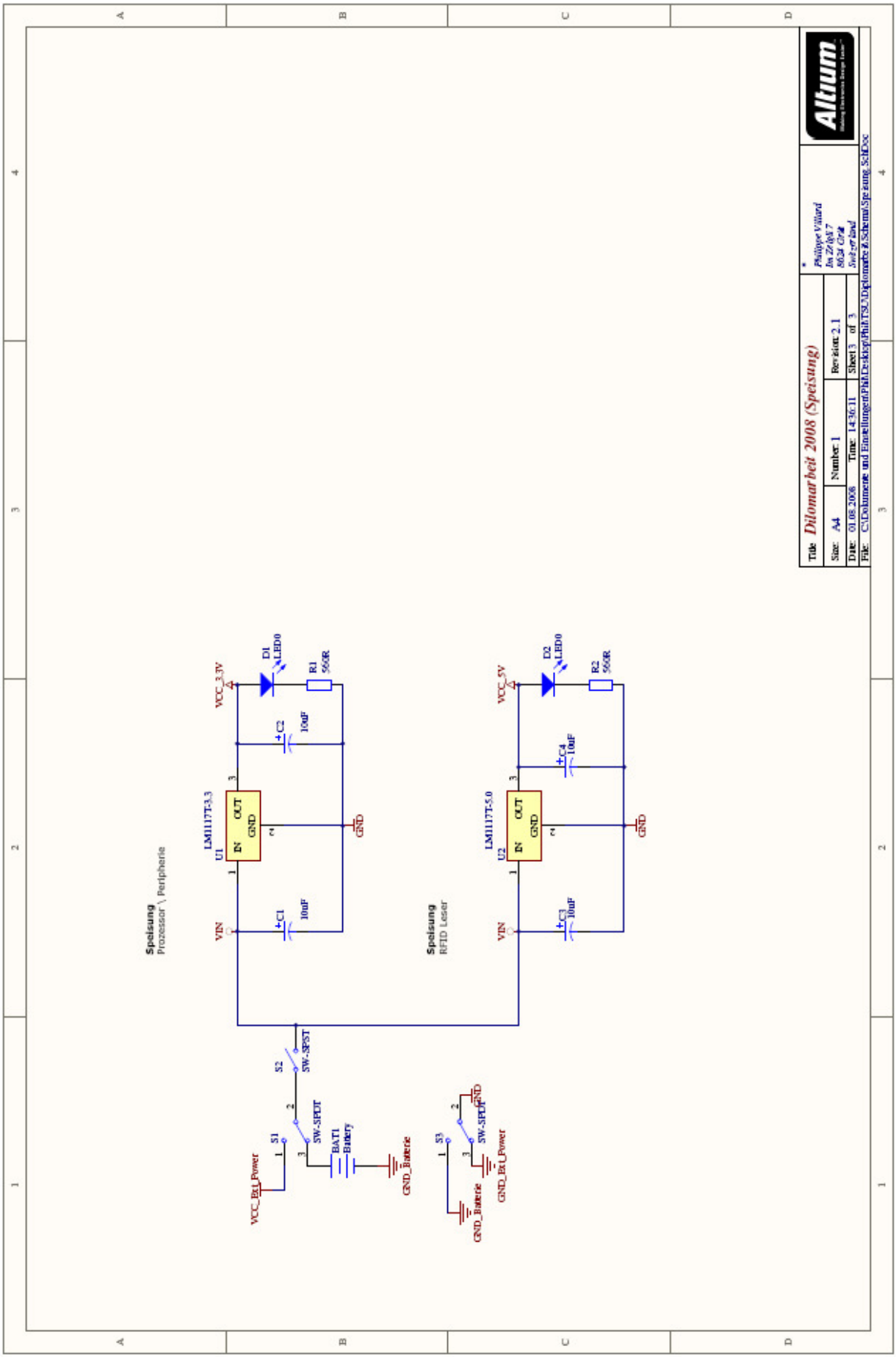
12.3.1 uC Anschlüsse



12.3.2 Peripherie



12.3.3 Speisung



12.4 Erklärungen zum Schema

Das Schema ist in 3 Bereiche aufgeteilt: uC Anschlüsse, Peripherie und Speisung.

uC Anschlüsse: Hier werden die direkten Anschlüsse an den uC veranschaulicht. Vorhandene Verbindungen des Header Board sind rot eingezeichnet.

Peripherie: Die Peripheriekomponenten sind in diesem Bereich des Schemas eingezeichnet. Da es für die Matrixtastatur keine Vorlage gab, wurde sie konventionell aufgezeichnet.

Speisung: Die Speisung umfasst 2 Linearregler LM1117. Beides sind Fixregler. Der eine liefert 3.3VDC, der andere 5VDC. Zur Umschaltung von Batteriebetrieb auf externe Speisung wurde ein Zweifachschalter eingesetzt. Um das korrekte Funktionieren der Speisung zu veranschaulichen werden grüne LEDs eingesetzt, welche bei vorhandener Spannung leuchten.

Die Stückliste zum Schema und die Gehäusezeichnung befinden sich im Anhang. Die Datenblätter der einzelnen Komponenten sind der CD am Ende der Dokumentation zu entnehmen.

12.4.1 Stromaufnahme

Gemessene Gesamtstromaufnahme mit Fluke 177 im Batteriebetrieb (9V)

Normalbetrieb (Gerät ist aufgestartet, keine Taste gedrückt): 161mA
Normalbetrieb (Gerät ist aufgestartet, keine Taste gedrückt, Tag in Feld): 172mA
Betrag schreiben (beim abwerten und laden): 208mA (spitze)
Betrag oder BNR lesen: 179mA (spitze)

12.4.2 Toleranzrechnung / Toleranzüberlegungen

Für die Realisation der Hardware mussten einzig bei der Speisung Überlegungen zur Toleranz gemacht werden. Als Eingangsspannung können 6.0-20VDC angeschlossen werden. Das ausgewählte Netzteil FW7333/12 von Friwo liefert 700mA bei 12VDC. Kühlkörper bei den Linearreglern sind eigentlich nicht notwendig, da die Regler nicht allzu heiss werden. Um einer schnellen Alterung vorzubeugen ist der 5V Regler mit einem Kühlkörper ausgestattet. Dies darum, weil der Leser davon gespiesen wird. Beim 3.3V Regler ist ein Kühlkörper nicht notwendig, der uC verbraucht zusammen mit dem Display und der Tastatur nur sehr wenig Energie.

13 Realisierung der Software

13.1 Grundsätzliches

Die Software des Kassensystems ist in der Programmiersprache "C" geschrieben und ist in verschiedene Module aufgeteilt. Jedes einzelne Modul beinhaltet verschiedene Funktionen. Grundsätzlich sind die Funktionsnamen möglichst authentisch mit der Funktion. Die einzelnen Funktionen werden nachfolgend kurz beschrieben. Der gesammte Quellcode befindet sich im Anhang oder auf der beiliegenden CD.

13.2 main

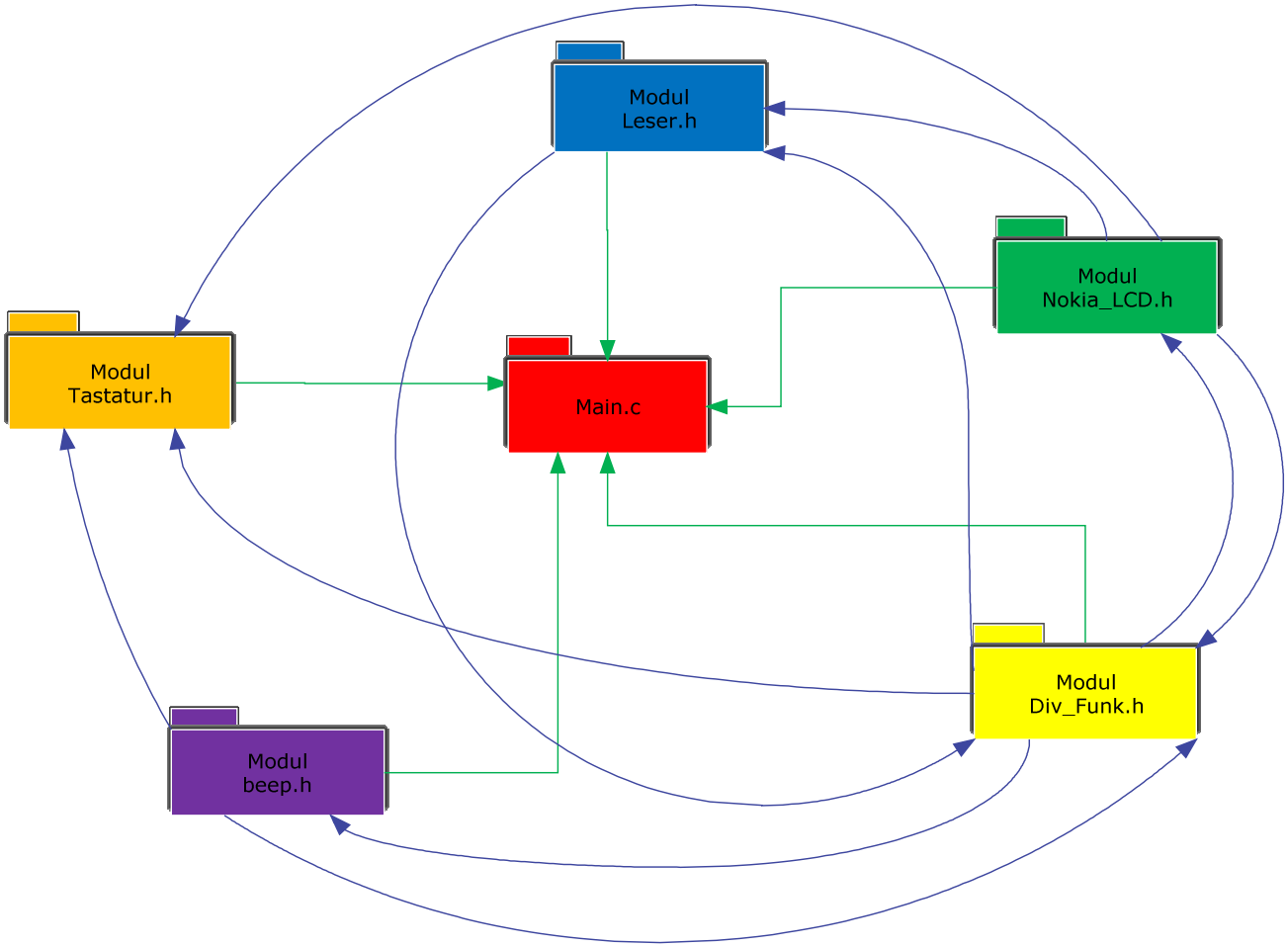


Abbildung 5: Übersicht main

13.3 Beep

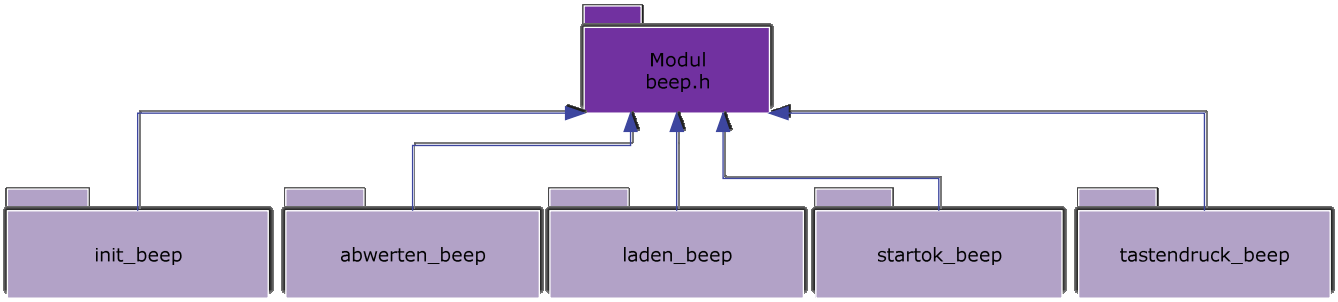


Abbildung 6: Übersicht beep

Das Modul beep dient zur Ansteuerung des Signalgebers.
Im Modul beep sind folgende Funktionen implementiert:

Funktion	Beschreibung
init_beep	Signalgeber und LED orange werden initialisiert (Port 2)
abwerten_beep	Ein Betrag wird abgezogen (akustisches Signal und LED löscht lange ab)
laden_beep	Ein Betrag wird abgezogen (akustisches Signal und LED leuchtet 3 mal auf)
startok_beep	Akustisches Signal, wenn Gerät bereit (Aufstartvorgang abgeschlossen)
tastendruck_beep	Kurzer Ton bei Tastendruck, Status LED kurz aus

Tabelle 15: Funktionen beep

13.4 Tastatur

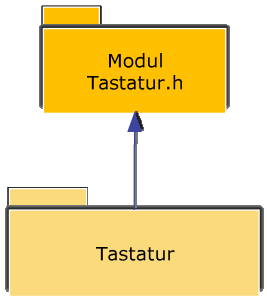


Abbildung 7: Übersicht Tastatur

Funktion	Beschreibung
Tastatur	Fragt permanent die Tastatur ab und gibt einen evtl. eingegebenen Betrag und den gedrückten FunktionKey (LADEN, ABWERTEN, ENTER, CLEAR, BNR Lesen und Betrag lesen) zurück. Sobald ein FunktionKey gedrückt wird, werden die Werte zurück gegeben. Ein Betrag muss also vor dem Drücken eines FunktionKey eingegeben werden. Sollen die einzelnen Tastendrücke sichtbar sein, so muss der Übergabeparameter Z_Ausgabe=1 sein.

Tabelle 16: Funktionen Tastatur

13.5 Nokia_lcd

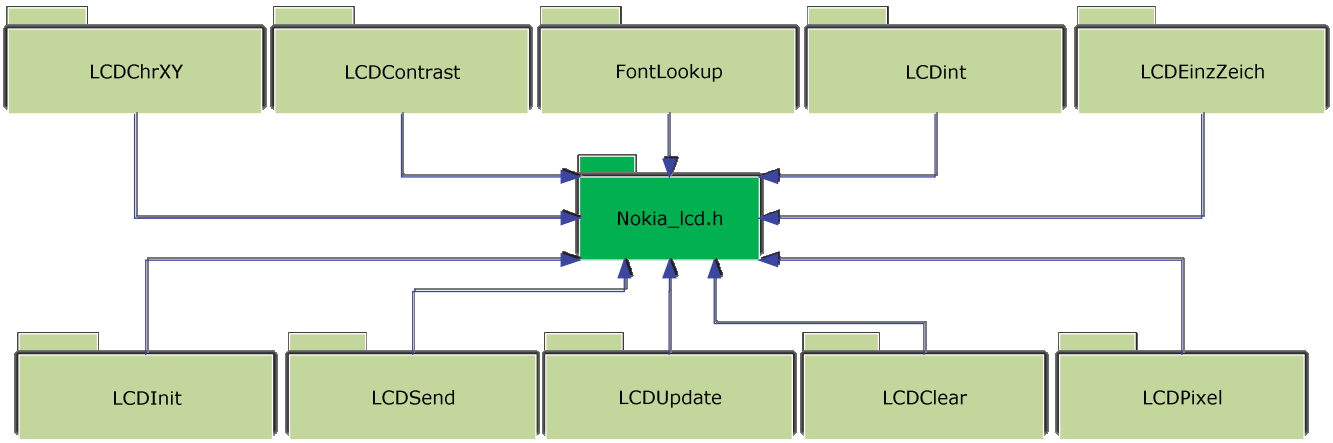


Abbildung 8: Übersicht Nokia_LCD

Funktion	Beschreibung
LCDInit	Initialisiert die SPI Schnittstelle für das LCD Display
LCDSend	Sendet ein Zeichen ans LCD Display
LCDUpdate	Updatet den Display Speicher
LCDClear	Löscht das LCD Display
LCDPixel	Einzelnes Pixel kann auf Display angezeigt werden
LCDChrXY	Einzelnes Zeichen auf Display ausgeben
LCDContrast	Kontrast des LCD Displays einstellen
LCDStr	String an LCD senden
LCDint	Integer an LCD senden
LCDEinzZeich	Zeigt eine einzelne integer Ziffer an

Tabelle 17: Funktionen Nokia_lcd

13.6 Div_Funk

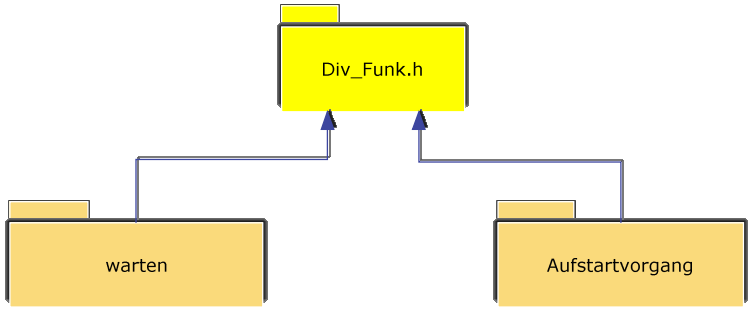


Abbildung 9: Übersicht Div_Funk

In diesem Modul sind zwei Funktionen enthalten:

Funktion	Beschreibung
warten	Einfache Warteschlaufe
Aufstartvorgang	Aufstartvorgang (LED, Display, Leser etc.)

Tabelle 18: Funktionen Div_Funk

13.7 Leser

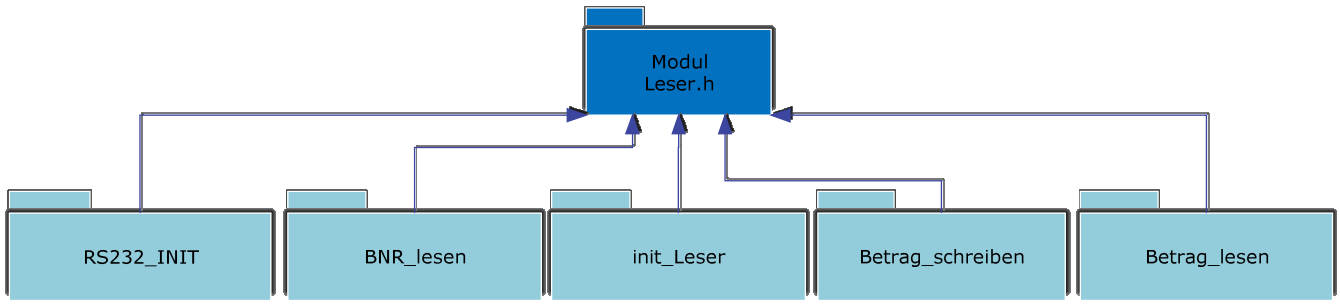


Abbildung 10: Übersicht Leser

Der Leser ist grundsätzlich "Slave". Um Informationen aus dem Leser zu holen, muss der Leser jeweils angefragt werden. Der Leser sendet die gewünschten Informationen nicht automatisch. Der Leser kann mit verschiedenen Schnittstellen arbeiten. Diese sind: RS232, RS485 oder I2C. Für den Einsatz im Kassensystem ist er für den RS232 Modus (9600-8-N-1) konfiguriert.
Im Modul Leser sind folgende Funktionen implementiert:

Funktion	Beschreibung
RS232_INIT	Die RS232 Schnittstelle des MSP430 wird mit einem Empfangsinterrupt initialisiert. RS232 Parameter: Bits Pro Sekunde: 9600; Datenbits: 8; Parität: Keine; Stoppbit: 1; Flussteuerung: Keine
init_Leser	Diese Funktion sendet dem Leser den Synchronisationsbefehl. Der Leser antwortet, wenn er bereit ist, mit seiner SW Release Nummer (z.B. G20040204). Diese wird am Display ausgegeben. Kommt keine Meldung zurück, so wird eine Fehlermeldung ausgegeben.
BNR_lesen	Der aktuelle Betrag eines Tags wird beim Leser angefragt. Ist ein Betrag vorhanden wird dieser zurückgegeben. Ansonsten wird eine Fehlermeldung ausgegeben.
Betrag_lesen	Der aktuelle Betrag eines Tags wird beim Leser angefragt. Ist ein Betrag vorhanden wird dieser zurückgegeben. Ansonsten wird eine Fehlermeldung ausgegeben.
Betrag_schreiben	Ein der Funktion übergebener Parameter Ladebetrag wird auf den Tag geschrieben. Bevor diese Funktion aufgerufen wird, muss ein Tag im Feld sein (kann z.B. mit Betrag_lesen geprüft werden).
speiloe_Leser	Diese Funktion sendet dem Leser den Befehl BNR lesen. Dieser Befehl wird benötigt, da der Leser evtl. noch alte Daten eines zum voraus gebrauchten Tags im Speicher hat.

Tabelle 19: Funktionen Leser

13.7.1 Befehl

Die Kommunikation vom "Master" zum "Slave" wird durch verschiedene Befehle realisiert. Es existieren Befehle für das Lesen der Benutzernummer, zur Synchronisation mit dem Leser, für das Lesen und Schreiben eines Geldbetrages und so weiter. Ein Befehl besteht aus der Befehlsnummer und 0 bis n Parametern. Die Befehlsnummer bestimmt die Funktion des Befehls, mit den Parametern werden die dazu nötigen Daten übergeben. Parameter können zum Beispiel den zu schreibenden Betrag oder die gewünschte zu lesende Nummer (Unikatsnummer, Serienummer oder Benutzernummer) sein.

Die Antwort des "Slave" ist im Prinzip gleich aufgebaut wie der Befehl des Master. Die Antwort des Slave erfolgt immer als Reaktion auf einen Befehl des Master. Konnte der korrekt empfangene Befehl ausgeführt werden, so erfolgt die Antwort durch Zurücksenden der gleichen Befehlsnummer, gefolgt von eventuell erforderlichen Informationen. Bei Fehlern beim Empfang des Befehls oder dessen Ausführung erfolgt die Rückmeldung mit einer speziellen Fehlerantwort.

13.8 Telegrammaufbau

Um die Befehle mit den Parametern übermitteln zu können wird diese Information in ein Telgramm umgewandelt.

13.9 Allgemein

Der Befehl wird in ein Telegramm umgewandelt, indem folgende Schritte durchgeführt werden. Wandlung der Parameter in Doppel-ASCII-Format (so ist es möglich, Werte von 0x00-0xFF zu übermitteln auch im 7 Bit Modus).

Beispiel: Parameter 0x3D ➔ 0x33 0x44

• Berechnen der Checksumme und anfügen im Doppel-ASCII-Format

Die Checksumme wird über folgende Daten gebildet:
• "Slave-Adresse" (sofern vorhanden)
• Doppel-ASCII-Werte der Parameter

Die Checksumme errechnet sich durch eine Exklusive-Oder-Verknüpfung dieser Werte. Die Checksumme wird in einen Doppel-ASCII-Wert gewandelt und an das Telegramm angeschlossen

Beispiel: Befehlnummer	Parameter	Checksumme
0x40	0x33 0x44	0x33 0x37

Die Parameter werden in Doppel-ASCII gewandelt. So ist es möglich Werte zwischen 0x00 und 0xFF zu übermitteln obwohl nur mit 7 Datenbits gearbeitet wird. Bei der Wandlung wird jedes "Nibble" (Halbbyte) in einen ASCII-Wert (‘0’..’9’;’A’..’F’) umgewandelt.

• Anhängen eines Schlusszeichens. (0x0d)

13.10 Beispiel Benutzernummer lesen

0x5D	// Befehl für Dat und ID Werte lesen
0x30	// Gewandelt in Doppel ASCII (0)
0x32	// Gewandelt in Doppel ASCII (2) BNR
0x35	// Gewandelt in Doppel ASCII (5) CRC
0x46	// Gewandelt in Doppel ASCII (F) CRC
0x0D	// CR

Auszugebendes Telegramm: 0x5D 0x30 0x32 0x35 0x46 (0x0D) ➔]025F(CR)

13.11 State Event Diagramm

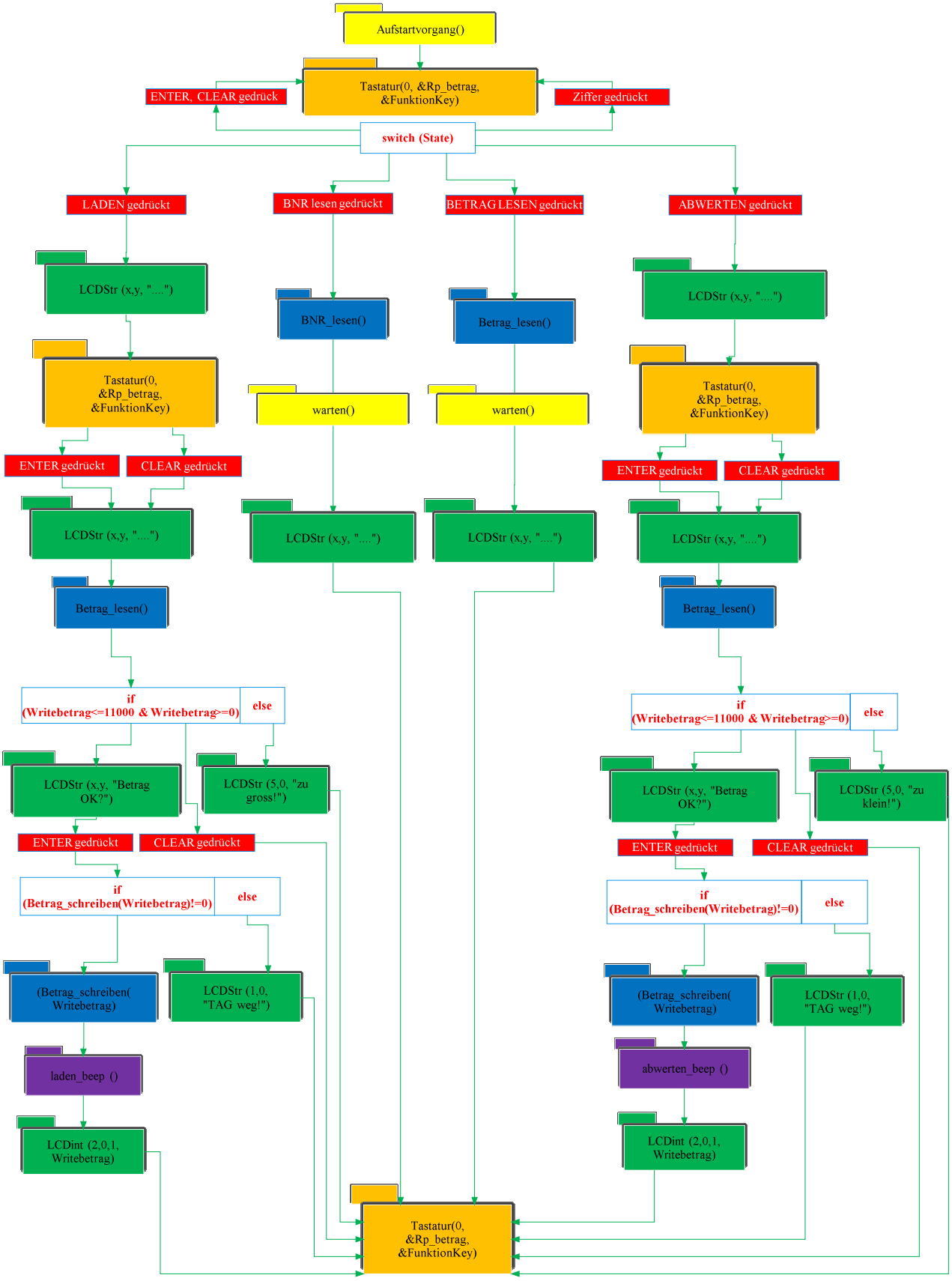


Abbildung 11: State Event Diagramm

14 Datensicherheit

14.1 Grundsätzliches

Bei Google werden beim Suchbegriff "RFID" 1.990.000 Treffer angezeigt, bei "RFID Sicherheit" 503.000 (suche Seiten auf Deutsch, Stand August 2008). Dies zeigt, dass das Thema Sicherheit in der RFID Welt immens wichtig ist. Das Thema Sicherheit hat viele Faktoren. Zum einen ist es die Sicherheit, dass die Daten korrekt und unverändert vom Leser zum Tag und umgekehrt gesendet werden, zum anderen ist Sicherheit auch mit der Privatsphäre verbunden. Denn wer möchte schon, dass die Firma bei der er angestellt ist (oder eine andere Institution) überprüfen kann, wer wann die Toilette benutzte oder mit dem Auto die Garageneinfahrt passierte (Zutrittskontrolle), wer wann einen Kaffee, einen Schokoriegel oder ein Mittagsmenü konsumiert hat (bargeldlose Bezahlung), wer welches Zugbillet gekauft hat oder wer wann bei einem Carsharing Unternehmen ein Auto von A nach B gefahren hat?

Sicherlich haben Sie auch schon von Sicherheit in der RFID Welt gehört. Sei es in einer Zeitung, einer Zeitschrift, im Internet oder im Fernsehen. In diesem Kapitel wird das Thema Sicherheit diversifiziert angeschaut. Es ist unterteilt in SW- bezogene Sicherheit und HW bezogene Sicherheit.

14.2 Software bezogene Sicherheit

14.2.1 Authenticity (Authentizität)

Gemäss Duden ist Authentizität folgendermassen definiert:
"Authentizität einer Information ist die sichere Zuordnung zum Sender und der Nachweis, dass die Informationen nach dem Versand nicht mehr verändert worden sind."
"Verfahren sollten sicherstellen, dass sowohl die Systemkomponenten (insbesondere die RFID-Tags) als auch die gespeicherten und übertragenen Daten eine gesicherte Herkunft besitzen, d.h. durch charakteristische Eigenschaften und einer eindeutigen Identität nachweislich authentisch und vertrauenswürdig sind. Gefälschte Komponenten oder Daten dürfen nicht akzeptiert werden, sondern sollten Fehlermeldungen auslösen."

Grundsätzlich besteht die Möglichkeit, auf einem Tag gespeicherte Daten oder vorhandene Applikationen durch Authentisierungsmechanismen zu schützen.

Die sehr flexible und offene LEGIC advant Technologie erfüllt gleichzeitig auch höchste Sicherheitsanforderungen. Um diesen beiden doch ziemlich gegensätzlichen Anforderungen zu entsprechen, wurden LEGIC Security Rules aufgestellt. Die Einhaltung der Security Rules wird kontinuierlich durch die Hardware und das sichere Leser-Betriebssystem (LEGIC OS) überwacht und sichergestellt. Elemente der Security Rules sind:

Autorisierungs- und Zugriffsmanagement (Master Token System Control)
– Regeln für die Berechtigung zum Initialisieren von Autorisierungs- und Applikationssegmenten
– Nur-Lese-Bereich (Schreibschutz)
– Schreib- und Leseschutz für Segmente und "Taufverfahren"
– Datenorganisation im Transponder
– Kommunikation über RF-Schnittstelle
– Physikalische Eigenschaften
– Antikollision
– Authentifizierung

Der Speicherbereich eines LEGIC Transponder ist aufgeteilt in einen Bereich für Transpondereigenschaften und in eines oder mehrere Segmente. In den Transpondereigenschaften befinden sich Transponder-Typ (User Media oder Master Media), HF-Standard und die Unikatsnummer, sowie die Grösse und Version des Dateisystems und die Art der Datenverschlüsselung.

Jeder Datenträger kann bis zu 127 Segmente (Applikationen) enthalten. Diese Segmente können sehr unterschiedlicher Art sein. Die von einem Autorisierungsmedium vererbten Daten werden als Stamp oder Stampdaten bezeichnet. Der Stamp stellt einen "Schlüssel" für die Berechtigung zum Initialisieren von weiteren Autorisierungs- und Applikationssegmenten oder für den Zugriff auf Segmentdaten dar. Der Stamp ist eine Segmentidentifikation und ist im Normalfall für die Art des Segments einmalig.

Über den Stamp kann ein Segment auf dem Datenträger gefunden werden. Eine Manipulation des Stamp ist nicht möglich, weil dieser nur mit Hilfe eines Autorisierungsmediums (AM) bei der Initialisierung geschrieben werden kann. Im Info Bereich des Segments befinden sich Informationen über die Lese- und Schreibberechtigungen. Es können Bereiche definiert werden, welche nur mit Authentifizierung beschrieben werden können. Damit ein Leser eine solche Authentifizierung bekommt, muss er "getauft" werden. Um Sicherheitsrisiken im Umgang mit bereits getauften LEGIC advant SM zu minimieren (z.B. Transport vom Lizenzpartner zum Installationsort), können LEGIC advant SM mit einem 4 Byte-Passwort geschützt werden. So können z.B. Taufdaten durch Unbefugte nicht ausgelesen werden. Passwortgeschützte LEGIC advant SM können im Feld nur aktiviert werden, wenn die Applikation nach jedem Power-up als erstes das entsprechende Kommando mit dem korrekten Passwort übermittelt. Nach drei falschen Passwörtern reagiert das SM nicht mehr und muss neu gestartet werden.

Für eine Taufe wird ein Taufmedium verwendet, welche speziell für dieses Segment hergestellt werden muss. Der Taufsatz ist dann im Leser gespeichert und könnte mit einer Enttaufkarte wieder gelöscht werden. Es können also nur Leser auf Datenträger schreiben (oder lesen), welche getauft sind.

Mit Hilfe einer Authentisierung können unautorisierte Lese- und Schreibzugriffe und missbräuchliche Verwendungen von Kill-Kommandos abgewehrt werden. Die so genannte "Challenge-Response-Methode" dient der Verhinderung von "Replay-Angriffen" (sich immer wiederholender Angriff)", da eine Zufallszahl immer nur für einen Authentisierungsvorgang gültig ist und somit derselbe Vorgang nicht durch erneutes Einspielen der vorher abgehörten Daten wiederholt werden kann.

Die Authentifizierung baut eine sichere Kommunikation zwischen LEGIC advant SM und Tag auf. Der Zugriff auf die LEGIC Datenstruktur (ausser Unikatsnummer) ist erst nach erfolgreicher Authentifizierung möglich. Der Authentifizierungsalgorithmus enthält eine Zufallszahl, die Unikatsnummer des Tags und einen Geheimschlüssel (64 ... 96 Bit). Jeder Zugriff auf Transponderdaten erfolgt somit mit einem anderen Schlüssel. Die Authentifizierung stellt sicher, dass missbräuchlich abgehörte Daten nicht wieder eingespeist werden können oder dass weitere Tags im HF-Feld die Datenübertragung nicht beeinflussen können.

Um Schutz gegen Abhören der Daten zu erreichen, kann die Datenübertragung bei LEGIC advant Transpondern optional mit DES oder 3DES verschlüsselt werden. Dieser Schutz ist applikationsabhängig und wird beim Anlegen des entsprechenden Applikationssegmentes definiert. Für die DES/3DES Verschlüsselung wird ein LEGIC spezifischer Schlüssel verwendet. DES oder 3DES-Algorithmen werden verwendet, weil sie relativ leicht zu implementieren und effizient in der Ausführung sind. Beide Kommunikationspartner müssen über den gemeinsamen, geheimen Schlüssel verfügen, um miteinander kommunizieren zu können.

14.2.2 Correctness (Korrektheit)

Die Mechanismen zur Datenübertragung sollten sicherstellen, dass Daten nach Verlassen ihrer Quelle (z.B. nach dem Beschreiben oder Auslesen eines Tags) unverändert sind und nicht zufällig oder böswillig modifiziert oder gelöscht wurden. Die Daten müssen korrekt und vollständig übertragen und gespeichert werden. Sensitive Daten dürfen nicht unautorisiert und unbemerkbar manipulierbar sein.

Je nach Anwendung spielt weniger die Vertraulichkeit der Daten, sondern eher ihre Unversehrtheit und Unverfälschtheit eine Rolle. Zu diesem Zweck lassen sich mit ähnlichen Kryptomechanismen wie zur Verschlüsselung der Datenübertragung, die Daten auch mit einer kryptographischen Prüfsumme versehen, welche eine authentische Datenübertragung, mit der Überprüfbarkeit der Herkunft der Daten und der Garantie ihrer Manipulationsfreiheit sicherstellt. Hiermit können Replay- und Man-in-the-middle-Angriffe verhindert werden.

14.3 Hardware bezogene Sicherheit / Elektrische Sicherheit

Die Datenübertragung vom Leser zum Transponder erfolgt nach dem Prinzip der Amplitudenumtastung (ASK, Amplitude Shift Keying).

	ISO 14443 A	**IS15693**	**LEGIC RF Standard**
Trägerfrequenz	13,56 MHz	13,56 MHz	13,56 MHz
Modulation	ASK 100%	ASK 10 % oder ASK 100 %	ASK 100 %
Codierung	modified Miller	1 aus 4 oder 1 aus 256	PWM
Datenrate	106 kbps	26,48 kbps (1 aus 4) oder 1,65 kbps (1 aus 256)	12,5 kbps

Tabelle 20: Modulation Leser - Transponder

Die Datenübertragung vom Transponder zum Leser erfolgt nach dem Prinzip der Lastmodulation. Der Resonanzkreis im Transponder wird mit einer Modulationsfrequenz belastet. Das Sicherheitsmodul im Leser erkennt die Belastungsänderung und ermittelt daraus die gelesenen Daten.

	ISO 14443 A	**IS15693**	**LEGIC RF Standard**
Modulations-frequenz	847 kHz	423,75 kHz (1 Seitenband) oder 423,75 kHz und 484,28 kHz (2 Seitenbänder)	212 kHz
Codierung	Manchester	Manchester	NRZ
Datenrate	106 kbps	6,67 oder 26,69 kbps	10 kbps

Tabelle 21: Modulation Transponder - Leser

Mechanische Angriffe, so genannte "Denial-of-Service-Angriffe" können bei passiven RFID-Chips (d.h. solche ohne eigene Stromversorgung wie eben Legic) lediglich durch mechanische Schutzmaßnahmen unterbunden werden, zum Beispiel zurückbleibende Beschädigungen an der Ware bei Entfernung des Chips. Weitergehende Maßnahmen wie z.B. automatische Alarmauslösung sind bisher nur bei aktiven Chips mit eigener Stromversorgung möglich.

14.3.1 Privacy (Datenschutz)

Illegales unerlaubtes Auslesen und Abhören von RFID Anwendungen (durch Kriminelle oder Neugierige) ist eine Problematik, die sich im Bereich der Identifizierung stellt. Unbemerktes Auslesen oder Auswerten kann aber in einem gewissen Bereich auch legal sein, zum Beispiel durch Läden, Konzerne, Behörden oder Betriebe. Dabei ist vor allem wichtig, dass Transparenz gewahrt wird. Eine gewisse Kontrolle durch den Staat (Datenschutz) ist unabdingbar.

Bei der Speicherung von Daten auf einem Tag kann sich in mehrfacher Hinsicht eine spezifische Bedrohungslage ergeben. Bedrohungen können zum Beispiel sein: die Verfügbarkeit von Daten, deren Integrität, Vertraulichkeit und Authentizität.

Gefahren werden aber auch oft zu hoch eingeschätzt, die technischen Möglichkeiten werden zum Teil zu stark überschätzt. Möglicherweise durch den Konsum von Agentenfilmen... Dennoch sind Trends vorhanden, zum Beispiel im Einzelhandel (Kundenkarten), bei Behörden (Terrorismus, Asylbetrug, Sozialschmarotzer) die Technologie zu missbrauchen. RFID muss deshalb sinnvoll eingesetzt werden.

Technische Innovationen wie RFID unterstützen Menschen dabei, ihren Alltag sicherer, einfacher und effizienter zu gestalten. Die Technologie ermöglicht es, Objekte mit Daten zum Beispiel mit einem EDV-System zu verknüpfen. Informationen zu Produkten lassen sich einfach und automatisch erfassen. Dies eröffnet ein breites Spektrum neuer Applikationen. Die Kritiker befürchten, dass mit der zunehmenden Verbreitung von RFID personenbezogene Daten unbemerkt und ohne Zustimmung der Betroffenen erhoben werden könnten. Aus diesem Grund sind Datensicherheit und das Recht auf Selbstbestimmung der Informationen wichtige Themen im Zusammenhang mit der Verwendung der Technologie.

Bei den meisten Anwendungen wie beispielsweise in der Logistik oder Produktionssteuerung werden personenbezogene Daten gar nicht erhoben. Es gibt aber auch Einsatzgebiete von RFID, bei denen personenbezogene Daten verarbeitet werden. Dazu zählen beispielsweise Zutrittskontrollen oder Mitgliederkarten in Fitnessclubs. Bei einem Einsatz von RFID in Supermärkten werden personenbezogene Daten nur erhoben, wenn der Kunde eine Kundenkarte (Cumulus / Supercard werden heute noch mit Strichcode betrieben) benutzt.
Wann immer personenbezogene Daten gespeichert werden, findet das Datenschutzgesetz (Schweizerisches Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)) Anwendung. Es verpflichtet Unternehmen, die persönliche oder personenbezogene Daten erheben oder verarbeiten, die betroffenen Personen über den Vorgang zu informieren und ihre Einwilligung einzuholen. Wenn eine solche vorliegt, kann sie vom Anwender jederzeit widerrufen werden. Die bestehenden datenschutzrechtlichen Vorgaben sind technologieneutral und stellen daher auch für Technologien wie RFID den datenschutzkonformen Einsatz sicher.

14.3.2 Emmission (Emissionen)

Das Legic advant Chipset 2560 wurde mit den Anforderungen nach EN 300330-1 V1.3.2 (2002-12) und den Anforderungen nach EN 301489-1 V1.4.1 (2002-08) geprüft.

Das HF Feld, welches durch einen Legic Leser generiert wird, ist relativ gering. Legic arbeitet vor allem im Proximity Bereich, das heisst im Bereich von wenigen cm. Deshalb sind Emissionen auf das weitere Umfeld relativ gering, auch wenn das HF Feld auch im Abstand von ca. einem Meter noch messbar ist.

14.3.3 Immission (Imissionen)

Einfluss	Auswirkung	Sicherheitselement
Störung des HF Felds	Fehlerhafte Datenübertragung	Prüfung der Datenintegrität mit CRC und MAC
Mehrere Transponder im HF Feld	Datenkollision	Antikollision, Authentifikation
Abhören von Daten	Missbräuchliche Verwendung von Daten	Datenverschlüsselung (DES, 3 DES)
Wiedereinspeisen von Daten	Missbräuchliche Verwendung von Daten	Authentifikation, MAC
Vorzeitiges Verlassen des HF Felds	Fehlerhafte Transaktion	Schattenspeicher

Tabelle 22: Einflüsse auf die Legic Applikation

Abhängig vom eingesetzten Frequenzband sind Störquellen für die eingesetzte RFID-Technik zu identifizieren und gegebenenfalls entsprechend zu schirmen.
Wichtig ist, dass Antennen von RFID Applikationen nicht auf Metallischen Oberflächen montiert werden, da sie sonst zu unvorhersehbaren Reflektionen oder sogar Verstärkungseffekten führen können.

15 Test / Messung / Verifikation

15.1 Testkonzept

Ein strukturiertes Testkonzept hinsichtlich der Aufgabenstellung, der zu erwartenden Messresultate und Spezifikationen und kritischer Punkte ist unabdingbar.

15.1.1 Relevante Messgrössen / Parameter mit Toleranzen

Das Testen der HW kann zum grössten Teil durch das Testen der Software abgedeckt werden. HW- seitig muss nur die Speisung geprüft werden.

Das Testen der SW ist sehr wichtig, um mögliche Abstürze und Fehlfunktionen zu vermeiden. Es ist zu untersuchen was passiert, wenn am Gerät manipuliert wird. Mögliche Manipulationsversuche können sein:

- Drücken mehrerer Tasten gleichzeitig
- Schnelles, unkontrolliertes Bedienen der Matrixtastatur
- Datenträger beim Schreiben (Ladevorgang / Abwertevorgang) aus HF Feld entfernen
- Gerät beim Schreiben ausschalten

Zu testen sind vor allem auch die Abläufe. Was passiert, wenn in einem Modus plötzlich eine unterwartete Taste gedrückt wird?

15.1.2 Testbedingungen / Systemzustände

Für das Testen des Geräts sind keine speziellen Bedingungen notwendig. Das Gerät liegt auf einer flachen Unterlage. Die Umgebungstemperatur entspricht normaler Zimmertemperatur.

15.2 Testumsetzung

15.2.1 Testaufbau

Der Testaufbau ist sehr einfach, es werden keine speziellen Bedingungen benötigt.

15.2.2 Testgeräte

Für die Messung der Speisung wurde das Fluke 177 Multimeter mit der Serienummer 94720124 verwendet.

15.3 Testresultate

15.3.1 Gerät einschalten

Schritte	Erwartet	Realität	Test bestanden
ON / OFF Schalter drücken	1. Startbildschirm wird angezeigt 2. Leser startet 3. Leser erfolgreich gestartet 4. "Willkommen" wird angezeigt 5. Signalton ertönt 3 mal 6. LED orange leuchtet 3 mal auf 7. Hauptmenu wird angezeigt	1. Startbildschirm wird angezeigt 2. Leser startet 3. Leser erfolgreich gestartet 4. "Willkommen" wird angezeigt 5. Signalton ertönt 3 mal 6. LED orange leuchtet 3 mal auf 7. Hauptmenu wird angezeigt	✓

Tabelle 23: Test Gerät einschalten

15.3.2 Test BNR Lesen

Schritte	Erwartet	Realität	Test bestanden
BNR LESEN drücken Tag in HF Feld	1. BNR wird angezeigt 2. Hauptmenu wird automatisch nach 3 Sekunden wieder angezeigt	1. BNR wird angezeigt 2. Hauptmenu wird automatisch nach 3 Sekunden wieder angezeigt	✓
BNR LESEN drücken Tag nicht in HF Feld	1. "Kein Tag da" wird angezeigt 2. Hauptmenu wird automatisch nach 3 Sekunden wieder angezeigt	1. "Kein Tag da" wird angezeigt 2. Hauptmenu wird automatisch nach 3 Sekunden wieder angezeigt	✓

Tabelle 24: Test BNR Lesen

15.3.3 Test Betrag lesen

Schritte	Erwartet	Realität	Test bestanden
BETRAG LESEN drücken Tag in HF Feld	1. Betrag wird angezeigt 2. Startbildschirm wird automatisch nach 3 Sekunden wieder angezeigt	1. Betrag wird angezeigt 2. Startbildschirm wird automatisch nach 3 Sekunden wieder angezeigt	✓
BNR LESEN drücken Tag nicht in HF Feld	1. "Kein Tag da" wird angezeigt 2. Hauptmenu wird automatisch nach 3 Sekunden wieder angezeigt	1. "Kein Tag da" wird angezeigt 2. Hauptmenu wird automatisch nach 3 Sekunden wieder angezeigt	✓

Tabelle 25: Test Betrag lesen

15.3.4 Test Clear

Schritte	Erwartet	Realität	Test bestanden
CLEAR drücken im Hauptmenu	1. Signalton ertönt wie bei Aufstartvorgang 2. LED orange leuchtet 3 mal auf 3. LCD wird initialisiert 4. Hauptmenu wird angezeigt	1. Signalton ertönt wie bei Aufstartvorgang 2. LED orange leuchtet 3 mal auf 3. LCD wird initialisiert 4. Hauptmenu wird angezeigt	✓
CLEAR wird im LADEN Modus gedrückt	1. Hauptmenu wird angezeigt	1. Hauptmenu wird angezeigt	✓
CLEAR wird im "ABWERTEN Modus" gedrückt	1. Hauptmenu wird angezeigt	1. Hauptmenu wird angezeigt	✓
CLEAR drücken im "BETRAG LESEN Modus"	1. Keine Funktion	1. Keine Funktion	✓
CLEAR drücken im "BNR Lesen Modus"	1. Keine Funktion	1. Keine Funktion	✓

Tabelle 26: Test Clear

15.3.5 Test Laden

Schritte	Erwartet	Realität	Test bestanden
LADEN wird gedrückt	1. Bildschirm "Rappenbetrag eingeben" wird angezeigt	1. Bildschirm "Rappenbetrag eingeben" wird angezeigt	✓
Rappenbetrag wird eingegeben: 1234	Jede Ziffer wird mit Signalton bestätigt und angezeigt	Jede Ziffer wird mit Signalton bestätigt und angezeigt	✓
Es wird eine andere Funktions- Taste als ENTER gedrückt	1. "Betrag laden?" wird angezeigt	1. "Betrag laden?" wird angezeigt	✓
Es werden mehr als 5 Ziffern eingegeben	1. ERROR_EINGABE erscheint	1. ERROR_EINGABE erscheint	✓
Variante 1: Betrag kleiner als 110.00 SFr. ENTER wird gedrückt	1. "Betrag laden?" wird angezeigt	1. "Betrag laden?" wird angezeigt	✓
Variante 2: Betrag würde grösser als 110.00 SFr. ENTER wird gedrückt	1. "Betrag wird zu gross!" wird angezeigt 2. Nach 2 Sekunden wird wieder das Hauptmenu angezeigt	1. "Betrag wird zu gross!" wird angezeigt 2. Nach 2 Sekunden wird wieder das Hauptmenu angezeigt	✓
ENTER wird gedrückt, Tag in HF Feld	1. Signalton ertönt kurz 3 mal 2. LED orange leuchtet 3 mal auf 3. Korrekter "Neuer Betrag:" wird 3 Sekunden lang angezeigt 4. Hauptmenu wird angezeigt	1. Signalton ertönt kurz 3 mal 2. LED orange leuchtet 3 mal auf 3. Korrekter "Neuer Betrag:" wird 3 Sekunden lang angezeigt 4. Hauptmenu wird angezeigt	✓
CLEAR wird gedrückt	1. Signalton ertönt wie bei Aufstartvorgang 2. LED orange leuchtet 3 mal auf 3. LCD wird initialisiert 4. Hauptmenu wird angezeigt	1. Signalton ertönt wie bei Aufstartvorgang 2. LED orange leuchtet 3 mal auf 3. LCD wird initialisiert 4. Hauptmenu wird angezeigt	✓
Es wird eine andere Funktions- Taste als ENTER gedrückt	1. Signalton ertönt wie bei Aufstartvorgang 2. LED orange leuchtet 3 mal auf 3. LCD wird initialisiert 4. Hauptmenu wird angezeigt	1. Signalton ertönt wie bei Aufstartvorgang 2. LED orange leuchtet 3 mal auf 3. LCD wird initialisiert 4. Hauptmenu wird angezeigt	✓
ENTER wird gedrückt, kein Tag in HF Feld	1. "Tag weg!" wird 3 Sekunden lang angezeigt 2. Hauptmenu wird angezeigt	1. "Tag weg!" wird 3 Sekunden lang angezeigt 2. Hauptmenu wird angezeigt	✓

Tabelle 27: Test Laden

15.3.6 Test Abwerten

Schritte	Erwartet	Realität	Test bestanden
ABWERTEN wird gedrückt	1. Bildschirm "Rappenbetrag eingeben" wird angezeigt	1. Bildschirm "Rappenbetrag eingeben" wird angezeigt	✓
Rappenbetrag wird eingegeben: 1234	Jede Ziffer wird mit Signalton bestätigt und angezeigt	Jede Ziffer wird mit Signalton bestätigt und angezeigt	✓
Es wird eine andere Funktions- Taste als ENTER gedrückt	1. "Betrag laden?" wird angezeigt	1. "Betrag laden?" wird angezeigt	✓
Es werden mehr als 5 Ziffern eingegeben	1. ERROR_EINGABE erscheint	1. ERROR_EINGABE erscheint	✓
Variante 1: Betrag wird grösser als 0.00 SFr. ENTER wird gedrückt	1. "Betrag abwerten?" wird angezeigt	1. "Betrag abwerten?" wird angezeigt	✓
Variante 2: Betrag würde kleiner als 0.00 SFr. ENTER wird gedrückt	1. "Betrag wird zu klein!" wird angezeigt 2. Nach 2 Sekunden wird wieder das Hauptmenu angezeigt	1. "Betrag wird zu klein!" wird angezeigt 2. Nach 2 Sekunden wird wieder das Hauptmenu angezeigt	✓
ENTER wird gedrückt, Tag in HF Feld	1. Signalton ertönt kurz 3 mal 2. LED orange leuchtet 3 mal auf 3. Korrekter "Neuer Betrag:" wird 3 Sekunden lang angezeigt 4. Hauptmenu wird angezeigt	1. Signalton ertönt kurz 3 mal 2. LED orange leuchtet 3 mal auf 3. Korrekter "Neuer Betrag:" wird 3 Sekunden lang angezeigt 4. Hauptmenu wird angezeigt	✓
CLEAR wird gedrückt	1. Signalton ertönt wie bei Aufstartvorgang 2. LED orange leuchtet 3 mal auf 3. LCD wird initialisiert 4. Hauptmenu wird angezeigt	1. Signalton ertönt wie bei Aufstartvorgang 2. LED orange leuchtet 3 mal auf 3. LCD wird initialisiert 4. Hauptmenu wird angezeigt	✓
Es wird eine andere Funktions- Taste als ENTER gedrückt	1. Signalton ertönt wie bei Aufstartvorgang 2. LED orange leuchtet 3 mal auf 3. LCD wird initialisiert 4. Hauptmenu wird angezeigt	1. Signalton ertönt wie bei Aufstartvorgang 2. LED orange leuchtet 3 mal auf 3. LCD wird initialisiert 4. Hauptmenu wird angezeigt	✓
ENTER wird gedrückt, kein Tag in HF Feld	1. "Tag weg!" wird 3 Sekunden lang angezeigt 2. Hauptmenu wird angezeigt	1. "Tag weg!" wird 3 Sekunden lang angezeigt 2. Hauptmenu wird angezeigt	✓

Tabelle 28: Test Abwerten

15.4 Interpretation der Testresultate / Konsequenzen

Die Testresultate zeigen, dass alle Tests erfolgreich durchgeführt worden sind.

15.5 Batterielebensdauer

Die Batterielebensdauer kann anhand der Gesamtstromaufnahme des Gerätes und der verwendeten Batterie berechnet werden:

Batteriespannung: 9V
Durchschnittliche Stromaufnahme: 178mA

Hersteller	Typ	Kapazitätsangabe [mAh]	theoretische Lebenserwartung[h]
Duracell®	Alkaline PLUS 6LR61/9V	680mAh	3.8
Varta	Longlive Extra 6LR61/9 V	550mAh	3.1
Energizer	Alkali/Mangan 6LR61/9V	625mAh	3.5

Diese Berechnungen hängen natürlich mit der Anzahl Transaktionen zusammen. Dazu kommt, dass ein Datenträger im Feld einen wesentlich höheren Stromverbrauch verursacht und somit die Batterielebens-dauer ebenfalls beeinflusst.
Ein Dauertest (Gerät permanent eingeschaltet, 50 Abwertungen, 50 Ladungen, 10 mal Betraglesen, 10 mal BNR lesen, Tag immer aus dem Feld, wenn keine Aktion) mit der oben genannten neuwertigen Duracell ergab eine Betriebsdauer von 4h und 10 Minuten.

15.6 Vergleich mit der Aufgabenstellung und Pflichtenheft

15.6.1 Gegenüberstellung der SOLL-IST-Grössen bzw. Parameter / Vergleich Mussziele

Beschreibung	SOLL	IST
Laden und Abwerten von Beträgen	Zwingend notwendig	Realisiert
Anzeige der Transaktionen auf einem Display	Zwingend notwendig	Realisiert
Eingabe der Geldbeträge über eine Tastatur	Notwendig	Realisiert
Erweiterbarkeit des Systems (elektrische Erweiterbarkeit, verschiedene Preiskategorien etc.)	Notwendig	Realisiert
Abklärungen betreffend Datensicherheit (Authenticity, Correctness, Privacy, Emmission, Immission)	Notwendig	Realisiert
Optische Darstellung (LED) über Betriebszustand	Nicht notwendig	Realisiert
Akustisches Signal bei einer Auf-/Abbuchung	Nicht notwendig	Realisiert

Tabelle 29: Gegenüberstellung SOLL / IST Mussziel

15.6.2 Gegenüberstellung der SOLL-IST-Grössen bzw. Parameter / Vergleich Wunschziele

Beschreibung	SOLL	IST
Logfile auf eine SD Karte	Wunschziel	Nicht realisiert ==> Zeitaufwand wäre zu gross gewesen. HW- mässig ist die SD Karte implementiert. Keine SW Implementation
Implementation Dateisystem um auf die SD Karte zu schreiben	Wunschziel	Nicht realisiert ==> Zeitaufwand
Anzeige Batteriezustand	Wunschziel	Nicht realisiert ==> Zeitaufwand

Tabelle 30: Gegenüberstellung SOLL / IST Wunschziele

15.6.3 Beurteilung und Fazit

Alle im Pflichtenheft geforderten Mussziele wurden realisiert. Sehr vorteilhaft wirkte sich die, im Nachhinein als kluge Entscheidung empfundene, Nichtrealisierung und softwaremässige Implementierung der SD Karte aus. Der Zeitaufwand wäre einfach zu gross gewesen und hätte unter Umständen die Mussziele gefährdet. Die Erweiterbarkeit des Systems durch den modularen SW Aufbau und die noch nicht gebrauchten Eingänge und Ausgänge des Mikroprozessors ist gewährleistet. Die SD Karte wurde HW- mässig eingebaut und müsste nur noch SW- mässig realisiert werden.

16 Die Zukunft des bargeldlosen Kassensystems

Eine Kommerzialisierung dieser Anwendung ist durchaus denkbar. Abnehmer wären zum Beispiel Gastrountenehmen mit Stammkunden wie zum Beispiel einem Club oder ähnlichem, wo jeder "Member" eine RFID Karte nicht nur zur Identifikation sondern auch zur bargeldlosen Bezahlung bekäme (Beispiel System in AlpenRock House™ am Flughafen Zürich: Mit der Strichkarte "HouseCheck" die man am Eingang erhält kann bis 200.- SFr. bezahlt werden, siehe auch http://www.alpenrock-house.com). Essen und Getränke könnten so ganz einfach und schnell bezahlt werden.
Natürlich bedürfte es bis zu einer Marktreife eines solchen Gerätes noch diverse Anpassungen. Es müsste ein Print gelayoutet werden, ein kostengünstigerer Typ des Mikrokontrollers MSP430 könnte evtl. auch verwendet werden, die 9V Batterie könnte durch einen Akku ersetzt werden, das Gehäuse könnte man bei Verwendung von SMD Komponenten noch kleiner gestalten. Zudem müsste der Displaykontrast von aussen einstellbar sein und eine Batterieanzeige müsste noch implementiert werden. Des Weiteren wäre eine sinnvolle Software- Einbindung des SD Kartenlesers unabdingbar, um eine Statistik über die verkauften Produkte zu führen.
All diese Erweiterungen und Einsparungen zusammengefasst, würde das Gerät ohne Leser ca. 50 SFr. kosten. Hinzu käme eine SD Karte (heutzutage ca. 10 SFr.) und der Leser, welcher beim Hersteller ca. 250 SFr. kosten würde. Die Produktionskosten kämen also deutlich unter 400 SFr. Wenn man beachtet, dass ein Kassensystem mit bargeldlosem Zahlungssystem auf dem Markt meistens weit über 2000 SFr. zu haben ist, wäre eine Rechnung für die Produktion eines solchen Gerätes zu überlegen.

17 Schlusswort

An einem der ersten Maitage dieses Jahres rannte ich an einem frisch gepflügten Acker vorbei. Es war einer der ersten Tage, nachdem ich die Aufgabenstellung zur Diplomarbeit erhalten hatte. Dieser Acker war für mich ein bisschen symptomatisch für den Beginn meiner Diplomarbeit. Auch er benötigt noch viel Arbeit bis zur Ernte.
Eine anstrengende, lehrreiche Zeit geht dem Ende entgegen. Bei dieser Diplomarbeit habe ich mir unglaublich viel Wissen angeeignet. Nicht nur was das Technische betrifft, sondern auch im projektspezifischen Arbeiten habe ich viel gelernt. Während meiner Diplomarbeit gab es immer wieder Hochs und Tiefs. Ein Höhepunkt war natürlich, als die ganze Hardware korrekt lief. Meine Freundin meinte zu meinem erfolgreichen Ansteuern des Display zwar nur lakonisch: „Das habe ich bei meinem Handy ja auch, das kann ja nicht so schwierig sein!“. Solche Kommentare wusste ich aber gekonnt zu überhören und meldete meinen Erfolg dann meinen Klassenkollegen über Skype, welche solche Leistungen aus meiner Sicht besser zu würdigen wussten.
Ein wichtiger Aspekt der Arbeit war auch, dass ich die Arbeit alleine und nicht in einem Zweierteam erstellte. Die Vor- und Nachteile gegenüber einer Teamarbeit waren ausgeglichen. So musste ich mich zum Beispiel nicht mit einer Person absprechen oder war nicht auf deren Termine angewiesen. Dafür konnte ich ein komplexeres Problem nicht oder nur beschränkt mit jemandem anderen besprechen, der sich dann auch motiviert für eine Lösungsfindung einsetzte. So war ich bei vielen Problemstellungen auf mich alleine gestellt und musste selbst eine Lösung finden. Dies trug dann natürlich ebenfalls zum Lerneffekt bei.

Als ich vor kurzem wieder dem Weg entlang rannte, wo im Mai der Acker lag, war keine braune Fläche mehr zu sehen. Stattdessen verwandelte er sich in der Zwischenzeit in ein riesiges, zwei Meter hohes Maisfeld mit unendlich vielen, gereiften Maiskolben. Das Gefühl, endlich fertig zu sein war äusserst angenehm.

18 Installations-/Montageanleitung

18.1 Allgemeines

Bevor das Gerät in Betrieb genommen wird, sind alle Dokumentationen in diesem Kapitel und das Kapitel "19 Bedienungsanleitung" durchzulesen.

18.2 Installation und Montage des Gerätes

Das Gerät ist am einfachsten auf einer ebenen Fläche (z.B. Tisch) bedienbar. Eine spezielle Montage des Gerätes ist nicht nötig. Das Gerät kann im Batteriebetrieb auch mobil benutzt werden.

18.2.1 Abgleich HF Feld

Um das HF Feld optimal abzugleichen ist ein Keramikschraubenzieher (damit das Feld nicht durch Metall gestört wird) und wenn möglich ein Feldmessgerät (Legic Powermeter) zu verwenden. Eine Abgleichanleitung befindet sich auf der Legic Homepage:
http://www.legic.com/de/download_statistics.html?content.filename=legic_standard_powermeter_20071218091436.pdf&content.cid=5620&content.lng=)
Ein Abgleich ist auch ohne Feldmessgerät möglich. Dazu muss der Kondensator immer ganz leicht (wenige Grad) gedreht werden. dann wird jeweils eine Lesung gemacht (z.B. BNR Lesen). Der Abgleichkondensator befindet sich auf der Antenne des Lesers (roter Drehkondensator), das Gerät ist also zu öffnen. Der Abgleich ist nur durch autorisierte Personen vorzunehmen.

19 Bedienungsanleitung

19.1 Allgemeine Informationen und Hinweise

- Verwenden Sie für den Betrieb des Gerätes ausschliesslich 6LR61/9V Batterien oder das zugehörige 12VDC Steckernetzgerät FW7333-12

- Das Gerät ist nicht wasserdicht, halten Sie es trocken.

- Sollte das Gerät verschmutzt sein, so kann es mit einem mit Fensterreiniger angefeuchteten Baumwolltuch abgerieben werden

- Das Gerät sollte nicht zu lange direkter Sonneneinstrahlung ausgesetzt werden

- Der maximale Betrag der auf den Datenträger aufgewertet werden kann beträgt 110.00 SFr.

- Kostenlosen Support erhalten Sie unter der E-Mailadresse: villard@gmx.ch

19.2 Inbetriebnahme

Das Gerät kann in zwei verschiedenen Betriebsarten betrieben werden:

Batteriebetrieb: Stellen Sie den Kippschalter auf Bat. und starten Sie das Gerät durch Drücken des schwarzen Drucktasters ON / OFF ein.

Netzbetrieb: Stellen Sie den Kippschalter auf Ext. und schliessen Sie das Steckernetzgerät FW7333-12 auf der rechten Seite des bargeldlosen Kassensystems an (Schraubverbindung). Anschliessend können Sie das Netzgerät an einer Steckdose anschliessen. Um das Gerät aufzustarten ist der schwarze Drucktaster auf der rechten Seite des Geräts zu drücken.

19.3 Bedienung

Das Gerät startet automatisch auf und zeigt während dem Startvorgang folgende Informationen an:

Abbildung 12: Anzeige Aufstartvorgang 1, 2, 3

Sobald das Gerät aufgestartet ist ertönt eine kurze Tonfolge (kurz-lang-kurz). Auf dem Display erscheint das Hauptmenu:

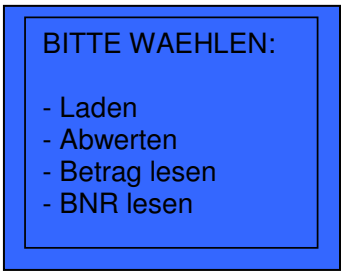


Abbildung 13: Anzeige Hauptmenü

Nun kann eine Funktion gewählt werden. Dies geschieht über die so genannten "FunktionKeys" LADEN, ABWERTEN, CLEAR, ENTER, BETRAG LESEN und BNR LESEN. Die Wahl muss über die Tastatur erfolgen.

19.3.1 LADEN und ABWERTEN

Die für diesen Prototypen eingesetzten Karten haben einen Maximalbetrag von 110.- SFr., können also nicht höher als dieser Betrag geladen werden. Der Maximalbetrag hängt von der Codierung der Tags ab. In diesem Beispiel wird von einem Tag mit 20.- SFr. Guthaben ausgegangen. Es werden 12.50 Sfr. geladen / abgewertet.

Nach dem Drücken von LADEN oder ABWERTEN zeigt das Display folgenden Inhalt:

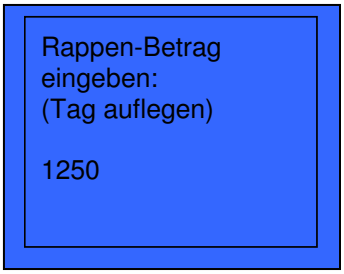


Abbildung 14: Anzeige LADEN / ABWERTEN

Ein Betrag (in Rappen) kann nun eingegeben werden. Danach ist die ENTER Taste zu drücken.

Wenn Sie den Vorgang abbrechen wollen, drücken Sie zwei Mal die CLEAR Taste. Sie kehren dann automatisch ins Hauptmenu zurück.

Folgender Bildschirm wird angezeigt:

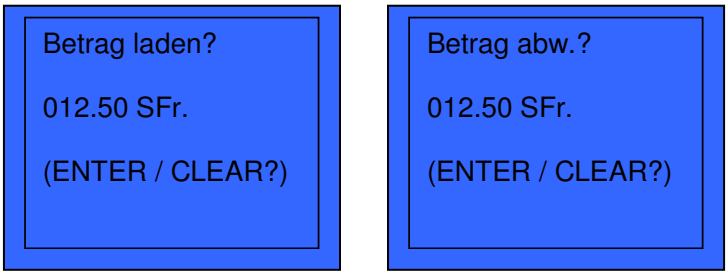


Abbildung 15: Anzeige LADEN / ABWERTEN?

Mit der Taste ENTER wird nun der Betrag geladen oder abgewertet, je nachdem, ob Sie zu Beginn LADEN oder ABWERTEN gewählt haben. Mit CLEAR gelangen Sie ins Hauptmenu zurück.

Stellen Sie sicher, dass sich ein Tag im HF Feld befindet!
Ansonsten wird eine Fehlermeldung angezeigt.

War die Transaktion erfolgreich, ertönen beim Laden 3 kurze Piepstöne hintereinander. Beim Abwerten ertönt ein einzelner langer Ton. Folgender Bildschirm wird angezeigt:

LADEN: ABWERTEN:

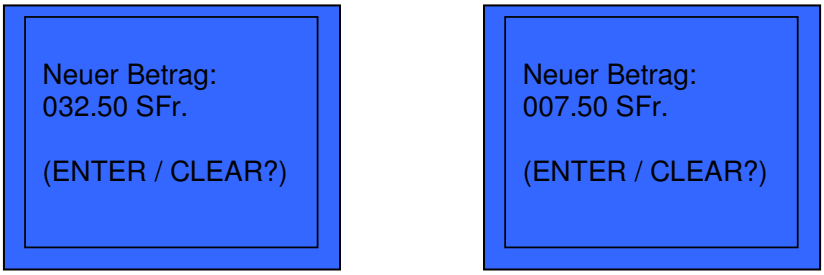


Abbildung 16: Anzeige neuer Betrag (LADEN / ABWERTEN)

19.3.2 CLEAR

Das Drücken der Taste CLEAR bringt Sie jeweils wieder ins Hauptmenü zurück. Es ertönt die gleiche Tonfolge wie beim Aufstartvorgang.

19.3.3 ENTER

Die ENTER Taste wird zur Eingabe von Beträgen benötigt.

19.3.4 BETRAG LESEN

Ist ein Datenträger im HF Feld, erscheint durch das Drücken der Tast BETRAG LESEN folgender Bildschirm:

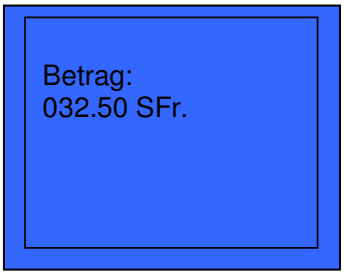


Abbildung 17: Anzeige Betrag

Ansonsten kommt eine Fehlermeldung.

19.3.5 BNR LESEN

Ist ein Datenträger im HF Feld, erscheint durch das Drücken der Tast BETRAG LESEN folgender Bildschirm:

Abbildung 18: Anzeige BNR

Ansonsten kommt eine Fehlermeldung.

Das Gerät ist nach bestem Wissen und Gewissen geprüft. Sollte dennoch ein Fehler angezeigt werden oder das Gerät nicht mehr reagieren, so starten Sie es durch zweimaliges Drücken des ON / OFF Schalters neu und melden Sie die Störung an: villard@gmx.ch.

19.3.6 Funktionsübersicht

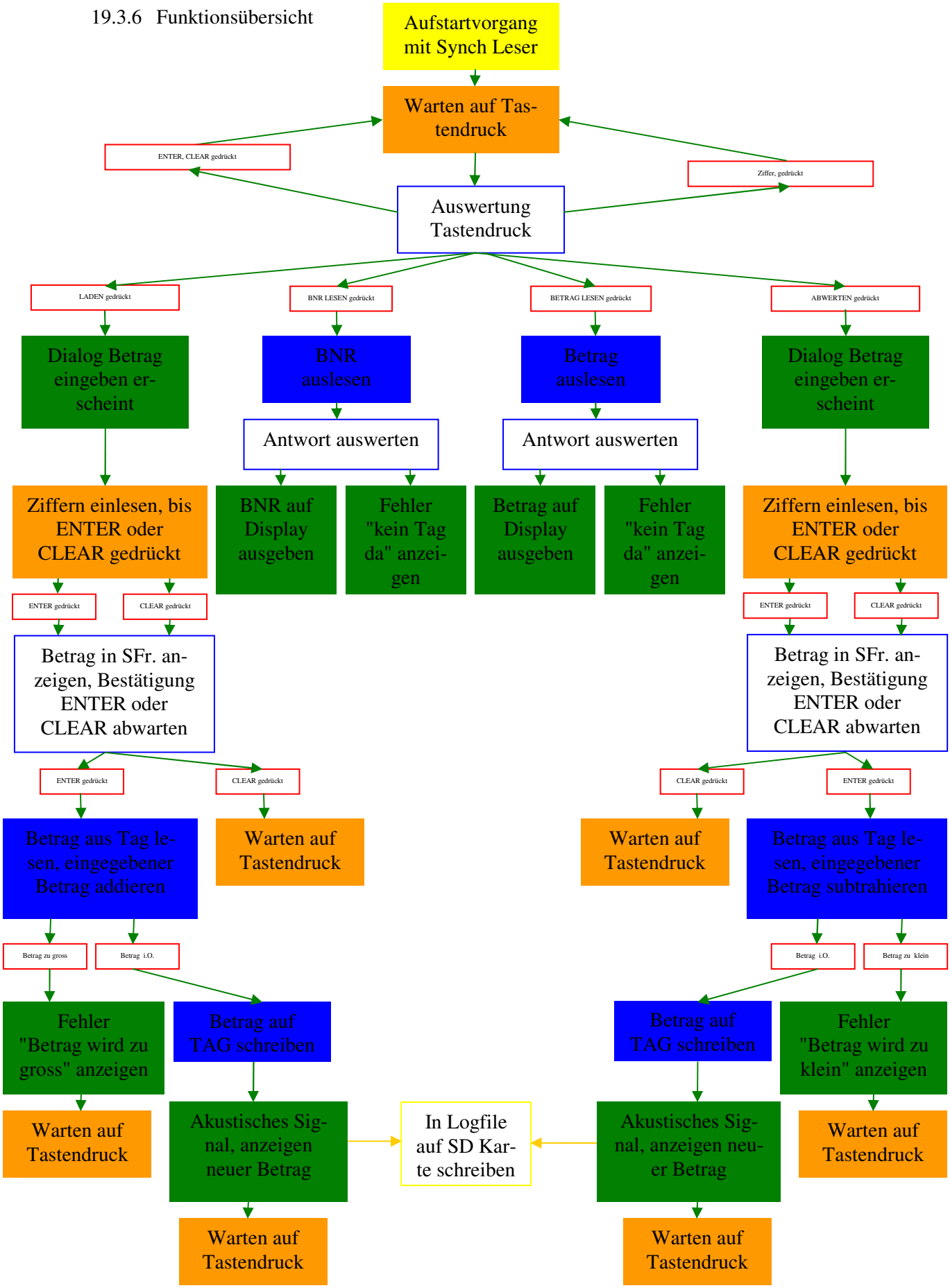


Abbildung 19: Funktionsübersicht

20 Glossar und Verzeichnisse

20.1 Glossar

DA	Diplomarbeit
RFID	Radio Frequency Identification
HFU	Höhere Fachschule Uster
Tag	Smart Card, Datenträger
Smart Card	Tag, Datenträger
Leser	RFID Schreib- / Leseeinheit
HW	Hardware
SW	Software
NFC	Near Field Communication
HF	Feld Hoch Frequenz Feld
SM	Security Modul
HF	High Frequency (Hochfrequenz)
CR	Carriage Return

20.2 Abbildungsverzeichnis

Abbildung 1: RFID -System 11
Abbildung 2: RFID Transponder (Tag) 12
Abbildung 3: Übersicht Hardware 12
Abbildung 4: Blockdiagramm 12
Abbildung 5: Übersicht main 12
Abbildung 6: Übersicht beep 12
Abbildung 7: Übersicht Tastatur 12
Abbildung 8: Übersicht Nokia_LCD 12
Abbildung 9: Übersicht Div_Funk 12
Abbildung 10: Übersicht Leser 12
Abbildung 11: State Event Diagramm 12
Abbildung 12: Anzeige Aufstartvorgang 1, 2, 3 12
Abbildung 13: Anzeige Hauptmenü 12
Abbildung 14: Anzeige LADEN / ABWERTEN 12
Abbildung 15: Anzeige LADEN / ABWERTEN? 12
Abbildung 16: Anzeige neuer Betrag (LADEN / ABWERTEN) 12
Abbildung 17: Anzeige Betrag 12
Abbildung 18: Anzeige BNR 12
Abbildung 19: Funktionsübersicht 12

20.3 Tabellenverzeichnis

Tabelle 1: Involvierte Personen 8
Tabelle 2: Vergleich Markt 12
Tabelle 3: Aufwandschätzung 12
Tabelle 4: Human↔Machine Interface Eingabe 12
Tabelle 5: Human↔Machine Interface Ausgabe 12
Tabelle 6: Mussziele 12
Tabelle 7: Wunschziele 12
Tabelle 8: Gesamtzeitplan 12
Tabelle 9: Zeitplan Realisierung 12
Tabelle 10: Konzeptvarianten 12
Tabelle 11: Evaluation Mikrokontroller 12
Tabelle 12: Evaluation Display 12
Tabelle 13: Evaluation Tastatur 12
Tabelle 14: Evaluation Entwicklungsumgebung 12
Tabelle 15: Funktionen beep 12
Tabelle 16: Funktionen Tastatur 12
Tabelle 17: Funktionen Nokia_lcd 12
Tabelle 18: Funktionen Div_Funk 12
Tabelle 19: Funktionen Leser 12
Tabelle 20: Modulation Leser - Transponder 12
Tabelle 21: Modulation Transponder - Leser 12
Tabelle 22: Einflüsse auf die Legic Applikation 12
Tabelle 23: Test Gerät einschalten 12
Tabelle 24: Test BNR Lesen 12
Tabelle 25: Test Betrag lesen 12
Tabelle 26: Test Clear 12
Tabelle 27: Test Laden 12
Tabelle 28: Test Abwerten 12
Tabelle 29: Gegenüberstellung SOLL / IST Mussziel 12
Tabelle 30: Gegenüberstellung SOLL / IST Wunschziele 12
Tabelle 31: Literaturverzeichnis 12
Tabelle 32: Beilagenverzeichnis 12

20.4 Quellenverzeichnis

20.4.1 Literaturverzeichnis

Titel	Autor	ISBN-10 Nummer
RFID & Co.	Harald Fischer	3-7723-5120-4
Mikrokontroller Programmierung (Script HFU)	Bruno Freitag / Martin Emmisberger / Matthias Kläy	-
Das grosse MSP430 Praxisbuch	Lutz Bierl	3-7723-4299-X
Einführung in die Kryptographie	Network Associates International / Phil Zimmermann	Keine
RFID-Studie 2007 Technologieintegrierte Datensicherheit bei RFID-Systemen	Deutsches Bundesministerium für Bildung und Forschung http://www.tzi.de/fileadmin/resources/publikationen/news/RFID-Studie_Final.pdf	Keine
Bundesgesetz über den Datenschutz	Bundesversammlung der Schweizerischen Eidgenossenschaft http://www.admin.ch/ch/d/sr/2/235.1.de.pdf	Keine

Tabelle 31: Literaturverzeichnis

20.4.2 Internetadressen

www.legic.com
www.olimex.com
www.distrelec.ch
www.hfu.ch
www.amontec.ch
www.wikipedia.ch

20.5 Stichwortverzeichnis

3DES 41
Amplitudenumtastung 42
Analyse des bestehenden Marktes 13
Anforderungen 16
Aufgabenstellung 6
Authenticity 40
Batch 11
Batteriebetrieb 54
Batterielebensdauer 49
Bedienung 55
Bedienungsanleitung 54
Befehl 37
Bestimmungen 7
Betreuer 8
Blockdiagramm 28
Checksumme 37
Correctness 42
Datensicherheit 40
DES 41
Display 25
Doppel ASCII 38
Elektronikarbeitsplatz 12
Emmission 43
Entwicklungsumgebung 17, 27
Frequenzband 44
Funktionsübersicht 58
GCC 27
Glossar 59
Grundlagen RFID 11
Hauptstudie 23
Header Board 23
HF Antenne 16
Hinweise 5
HMI 17
IAR 12, 27
Immission 44
Inbetriebnahme 54
Inhaltsverzeichnis 1
Installations-/Montageanleitung 53
Involvierte Personen 8
Konventionen 5
Kühlkörper 32
Legic Schreib- / Leseeinheit 5
Leser 36
Lösungsvorgehen 9
Luftschnittstelle 12
Machbarkeit 14
Management- Summary 9
Mikrokontroller 24
MSP430 24
Mussziele 19
Netzbetrieb 54
NFC 9
Peripherie 30
Persönliche Zielsetzungen 20
Pflichtenheft 16
Privacy 43
Privatsphäre 40
Programmiersprache 33
Prototyp 16
Proximity 43
Realisation 28
RFID Medium 5
Schema 29
Schlusswort 52
Schreib-/Leseeinheit 16
Segmente 41
Speicherbereich 41
Speisung 17, 31, 32
State Event Diagramm 39
Steckernetzgerät 54
Stromaufnahme 32
Tastatur 26
Taufe 41
Telegrammaufbau 37
Test 45
Toleranzüberlegungen 32
Transponder 12
Vorabklärungen 11
Wunschziele 19
Zeitplanung 21
Zukunft 51

21 Beilagen

21.1 Beilagenverzeichnis

Beilage	Titel
1	CD mit Programm / Datenblätter / Bilder / Dokumentation
2	Anhang mit Betreuungssitzungen / Gehäuseskizze / Stückliste / Quellcode

Tabelle 32: Beilagenverzeichnis

22 Daten CD